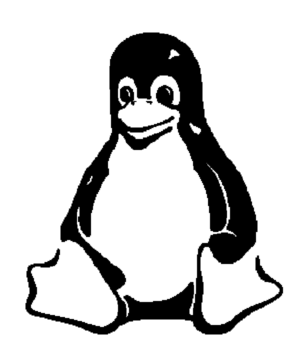


# Aufbau eines Kommunikationsservers mit Linux

Band 1: Schulungsunterlage

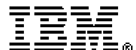
IBM®




**Impressum**

Dr. Björn Trösken (Vivex GmbH)
Werner Bill Schwenk (CSG – IBM Global Service Company)

Wir danken der Firma Vivex GmbH (Berlin) für die freundliche Unterstützung bei der Erstellung der Unterlagen






# Inhaltsverzeichnis


Multimedi@
Schule


Multimedi@
Schule

# 1 Einleitung

In diesem dreitägigen Kurs werden Sie lernen, mit Hilfe von Linux einen sogenannten Kommunikationsserver aufzubauen. Dieser Kommunikationsserver wird folgende Eigenschaften aufweisen:

- **Gateway + Masquerading:** verbindet das LAN mit dem Internet und versteckt lokale IP-Adressen
- **Name-Server:** löst Rechnernamen in IP-Adressen auf
- **Fileserver für Microsoft Windows Clients**: wird wie jeder andere Windows-Rechner durch Einsatz von "Samba" verwendet
- **Web-Server:** dient der Veröffentlichung eigener Informationen im Internet
- **FTP-Server:** ermöglicht die Dateiübertragung vom und zum Kommunikationsserver via FTP
- **Caching-Server:** beschleunigt den Zugang zu Internet-Informationen
- **Proxy-Server:** verhindert unberechtigte Zugriffe vom Internet ins LAN und umgekehrt
- **E-Mail-Server:** empfängt und versendet elektronische Post
- **News-Server:** stellt Nachrichten (News) bereit

## 1.1 Ziel dieser Schulung

Sie werden mit dem in diesem Kurs vermittelten Wissen in der Lage sein, ein eigenes lokales Netzwerk (LAN) ans Internet anzuschließen und die wichtigsten Internet-Dienste über geeignete Kontroll- und Sicherheitsmaßnahmen zu nutzen. Basis hierfür sind die Produkte S.u.S.E. Linux 5.2 sowie das Programmpaket Netscape Communicator.

## 1.2 Voraussetzungen

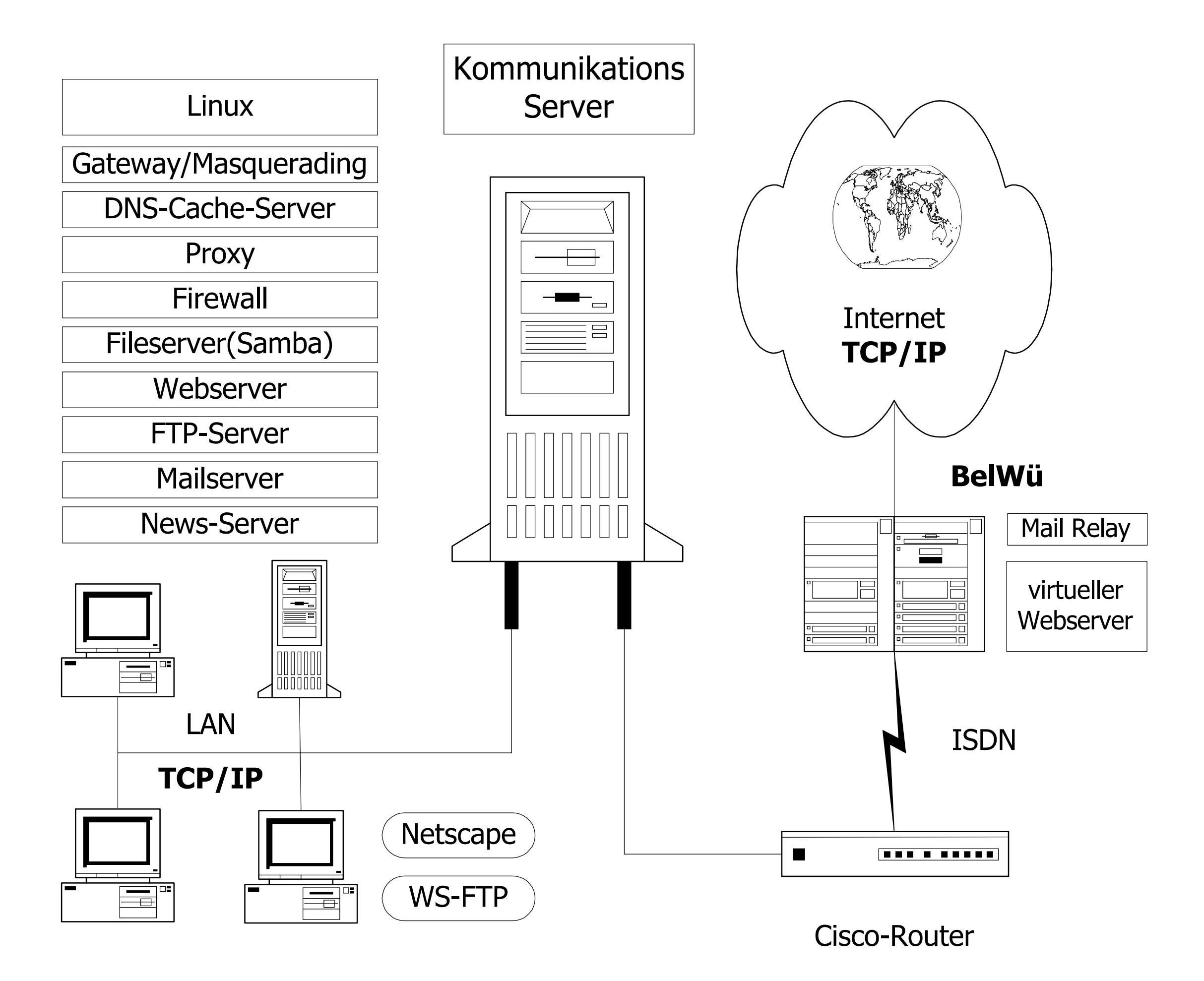
Dieser Kurs richtet sich an Administratoren, die am Linux-Grundkurs teilgenommen haben bzw. über gute Kenntnisse in der Verwaltung von Linux-Rechnern in Kombination mit Windows 95- bzw. Windows 3.11-Clients verfügen.

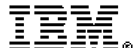





## 1.3 Übersicht über den Kursinhalt

Die folgende Übersicht skizziert die ideale Internetanbindung eines LANs über einen Kommunikations-Server. Alle genannten Dienste bzw. Produkte werden in diesem Kurs besprochen und installiert. Das Linux-Betriebssystem finden Sie in diesem Kurs bereits installiert vor, eine detaillierte Installationsanleitung finden Sie jedoch im Übungsteil.



# 2 Das Internet - Grundlagen und Gefahren

Die heutige Gesellschaft ist durch den Wandel zu einer Informationsgesellschaft geprägt. Die Ressource *Information* entwickelt sich neben Boden, Rohstoffen, Kapital und Arbeit zu einem der wichtigsten Wirtschaftsfaktoren. Als Folge des enormen Wachstums der reinen Informationsmenge ist ein Anstieg des Bedarfs zu verzeichnen, diese Informationen möglichst effektiv zu organisieren, zu verteilen und schneller zu transportieren.
Obwohl das Internet bereits seit über 25 Jahre existiert, ist es erst in den letzten Jahren in das Bewusstsein der Öffentlichkeit gerückt. Das Internet ist das einzige Medium, das nahezu grenzenlose Informations- und Kommunikationsmöglichkeiten bietet. Die steigenden Übertragungsbandbreiten lassen das Internet täglich mehr zum *Information-Highway* werden.
Ende der 50er Jahre erhielt die ARPA (Advanced Research Projects Agency), eine Abteilung des US-amerikanischen Verteidigungsministeriums, den Auftrag, einen Ersatz für die bis dahin verwendete leitungsorientierte Art der Datenübertragung zu entwickeln. Die leitungsorientierte Datenübertragung war sehr störanfällig und damit nicht sehr zuverlässig. Die ARPA entwickelte daraufhin eine paketorientierte Form der Datenübertragung. Bei dieser Art der Datenübertragung wird die Information in kleine Datenpakete aufgeteilt, die unabhängig voneinander einem Zielort übermittelt werden. Am Zielort werden diese Datenpakete wieder zur Information zusammengesetzt.
Als Folge dieser modernen Art der Datenübertragung startete Ende 1969 das *ARPAnet* als erstes paketorientiertes Netzwerk den Testbetrieb. Zu Beginn waren vier Universitäts- und Forschungsstandorte in den USA über Telefonleitungen miteinander verbunden. Im Laufe der Jahre entstanden neben dem ARPAnet weitere paketorientierte Netzwerke. Diese unterschiedlichen heterogenen Netzwerke wurden auf der Grundlage eines weiteren Forschungsauftrags Mitte der 70er Jahre miteinander verbunden. Das nun entstandene »Netz zwischen den Netzen« erhielt den Namen *Internet*. Eigens für das Internet wurde ein neues Übertragungsprotokoll, das TCP/IP, entwickelt. Mit der Umstellung aller Rechner im ARPAnet auf TCP/IP Anfang der 80er Jahre wurde dieses zum Standardübertragungsprotokoll erklärt. In dieser Zeit folgte die Aufteilung des sehr stark angewachsenen Netzes in einen rein militärischen und einen mehr forschungsorientierten Teil, aus dem das jetzt bekannte Internet hervorgeht.

## 2.1 Aufbau des Internets

Als Internet wird die Verbindung all jener Computer bezeichnet, die über Telefon- oder Standleitungen miteinander kommunizieren können. Das Internet präsentiert sich heute als Verbindung vieler, von verschiedenen Organisationen betreuter Teilnetze. Obwohl einzelne Organisationen bestimmte Aufgaben für das gesamte Internet erfüllen, gibt es jedoch keine Organisation, die für das Internet zuständig und verantwortlich ist. Die rasante Entwicklung des Internets basiert auf Impulsen der Betreiber von Teilnetzen und einzelner Benutzer. Der

Aufbau des Internets ist in der ganzen Welt identisch. Permanente Standleitungen verbinden als Hochgeschwindigkeitsverbindungen die Metropolen eines Kontinents miteinander. Diese Hauptverbindungsstrecken werden auch als Backbone-Netze bezeichnet. Die Kontinente sind über Transkontinentalkabel oder Satellitenstrecken miteinander verbunden.

Der deutsche Teil des Internets stützt sich im Wesentlichen auf Standleitungen der großen kommerziellen oder nicht kommerziellen Internet-Provider. Die Einwahlpunkte der Internet-Provider sind in der ganzen Bundesrepublik verteilt und wiederum mittels Standleitungen an die Zentralen der Internet-Provider angebunden. Firmen, Organisationen oder Privatpersonen können den Zugang zum Internet durch Anschluss an den Zugangspunkt des Internetproviders ihrer Wahl erhalten.




**Abbildung 2-1:** Die Standleitungen des XLINK in Deutschland

Die Anzahl der an das Internet angeschlossenen Hosts (=Computer im Internet) ist explosionsartig angestiegen, unterstützt durch die Kommerzialisierung des Internets.

Da niemand, außer den Systemadministratoren der angeschlossenen Netze, etwas über die Vergabe und tatsächliche Nutzung der IP-Adressen sagen kann, kann eine statistische Auswertung ausschließlich über Stichproben erfolgen. So werden von dem US-amerikanischen

Unternehmen Network Wizards regelmäßige Erhebungen mittels des Kommandos ping (eine Art Echolot im Internet) an ca. 1% aller Hosts durchgeführt. Bereits im Jahr 1990 bestand das Internet aus über 3.000 lokalen Netzwerken mit über 200.000 eingebundenen Hosts. Heute gibt es allein in Deutschland über eine Million und in Europa mehr als 5 Millionen Hosts im Internet.

## 2.2 Dienste des Internets

### 2.2.1 E-Mail

Im Internet gibt es verschiedene Formen des Informationsaustausches. Die **E-Mail (Electronic Mail)** ist ein Medium, ähnlich einem Brief, mit dem reine Textinformationen oder auch Dateien ausgetauscht werden können. Dies geschieht immer von einem „Briefkasten“ zum anderen. Grundvoraussetzung dafür ist also das Vorhandensein eines solchen „Briefkastens“, der sog. E-Mail-Adresse. Der Informationsaustausch ist dabei nicht nur auf die ungefähr 60 Mio. Internet-Teilnehmerinnen und -teilnehmer beschränkt. Hinzu kommen ungefähr weitere 30 Mio. E-Mailempfänger in anderen Netzen, wie z.B. usenet, fidonet, T-Online, CompuServe oder AOL, die über sog. Mail-Gateways an das Internet angebunden sind. Der Nachrichtenversand via E-Mail bietet viele Vorteile. E-Mails sind zum einen wesentlich schneller und zuverlässiger als ein Brief (in wenigen Sekunden um die Welt), zum anderen auch wesentlich kostengünstiger als ein Fax, da der Versand meist zum Telefon-Ortstarif (je nach Provider) erfolgen kann.

### 2.2.2 WWW

Ein weiteres Medium ist das **World Wide Web (WWW)**. Das WWW ist zwar nur ein Teil des Internet, dafür aber der Bekannteste. Das liegt mit Sicherheit an seiner bunten grafischen Oberfläche, mit der es eine Fülle von sogenannten Homepages anbietet. Bekannte Softwareriesen, Organisationen und Vereine aber auch private Anwender veröffentlichen im WWW ihre Websites.
Das WWW entstand erst 1990 im Kernforschungszentrum Cern (Schweiz) und erlöste die Anwenderinnen und Anwender von kryptischen Zeichen bei der Datenübertragung. Um das WWW nutzen zu können benötigt man eine entsprechende Software, einen sog. **Web-Browser**, der auf dem eigenen PC installiert sein muss. Die verbreitetsten Browser sind der *Netscape-Navigator* und der *Microsoft-Internet-Explorer*. Das WWW ermöglicht den Datenaustausch mittels sog. Hypertext. Hypertext ist ein System von Dokumenten, die durch Schlüsselwörter, auch *links* genannt, verkettet sind. In einem Hypertext sind Schlüsselwörter integriert, die von dem übrigen Text hervorgehoben sind. Die Hypertextverweise können mit der Maus angeklickt werden, um zum begehrten Ziel zu finden. Dabei ist es unerheblich, ob die Dokumente auf dem selben Server oder irgendwo anders in der Welt zu finden sind. Diese Möglichkeit wird auch von den Windows-Hilfsprogrammen genutzt. Der Nachteil von Hy-

pertext ist, dass man sich beim Hin- und Herklicken verzetteln und regelrecht „verlaufen" kann. Jedem Verweis folgt ein Verweis, der wiederum einen Verweis nach sich zieht usw.. Am Ende weißt man nicht mehr wo man angefangen hat, und was man überhaupt wollte.

#### 2.2.2.1 Web-Browser

Um das World Wide Web nutzen zu können, benötigt man einen sog**. Web-Browser**. Es sind eine Vielzahl von Web-Browsern im Internet frei verfügbar. Einige müssen käuflich erworben werden. Die zwei bekanntesten Web-Browser sind der Navigator (auch Communicator) von Netscape und der Internet-Explorer von Microsoft. Der Internet-Explorer liegt den aktuellen Windows-Versionen kostenlos bei. Der Navigator ist kostenlos im Internet verfügbar und kann via FTP heruntergeladen werden. Weitere Informationen über den Netscape-Browser finden Sie unter http://www.netscape.com/de und im Kapitel 5.4.

#### 2.2.2.2 Web-Server

Auf der Serverseite wird eine entsprechende Web-Server-Software benötigt. Auch hier sind eine Vielzahl von Produkten verfügbar. Die meisten davon sind allerdings ausschließlich käuflich zu erwerben. Es werden Web-Server von Microsoft, Netscape, Novell und anderen Firmen angeboten. Nähere Informationen über den NetWare-Web-Server von Novell finden Sie im Kapitel 7.
Im UNIX- bzw. Linux-Bereich ist die meiste Ware frei verfügbar, wie z.B. der Apache-Web-Server (http://www.apache.com), der weltweit einen Marktanteil von über 50% aufweist.

### 2.2.3 FTP

Der Internet-Dienst FTP (file transfer protocol) dient der Übertragung von Dateien zwischen zwei Internetrechnern. FTP stammt aus der UNIX-Welt und basiert auf dem Übertragungsprotokoll TCP/IP. Der Vorteil von FTP ist, dass Daten zwischen Rechnern unterschiedlicher Betriebssysteme mit den selben Befehlen und Vorgehensweisen ausgetauscht werden können. Der Benutzer muss sich bei der Benutzung von FTP keine Gedanken über betriebsspezifische Besonderheiten machen.
Das Internet stellt eine große Anzahl von FTP-Servern zur Verfügung, auf denen umfangreiche Datenarchive zu den unterschiedlichsten Themenbereichen bereitgestellt werden.
FTP stellt den Benutzern Befehle zur Verfügung, mit denen alle Aufgaben im Zusammenhang mit der Datenübertragung erledigt werden können. Moderne FTP-Programme, wie das im Internet verfügbare `WS_FTP`, arbeiten auf Windows-Basis und können deshalb mit der Maus bedient werden.

Vorgehensweise beim Datenaustausch mittels FTP:

1. Auswahl des gewünschten FTP-Servers.
2. Aufbau einer Verbindung
3. Eingabe der Benutzerkennung und eines Passwortes (s. **Abbildung 2-2**). Viele FTP-Server erlauben eine anonyme Anwendung (*anonymous*), d.h. die Dateien sind der Öffentlichkeit frei zugängig. In diesem Fall muss man als Benutzerkennung ***anonymous*** und als Passwort die eigene E-Mail-Adresse (z.B. ***name@server.de***) angeben.
4. Auswahl der gesuchten Datei mittels Mausklick (bei \`WS_FTP\`) oder Befehlen.
5. Starten der Datenübertragung mittels Mausklick (s. **Abbildung 2-3**) oder entsprechendem Befehl. Generell muss man aufpassen, welcher Dateityp (Text- oder Binärdatei) ausgewählt wird, weil es zu Problemen führen kann, wenn man eine Binärdatei als Textdatei überträgt.

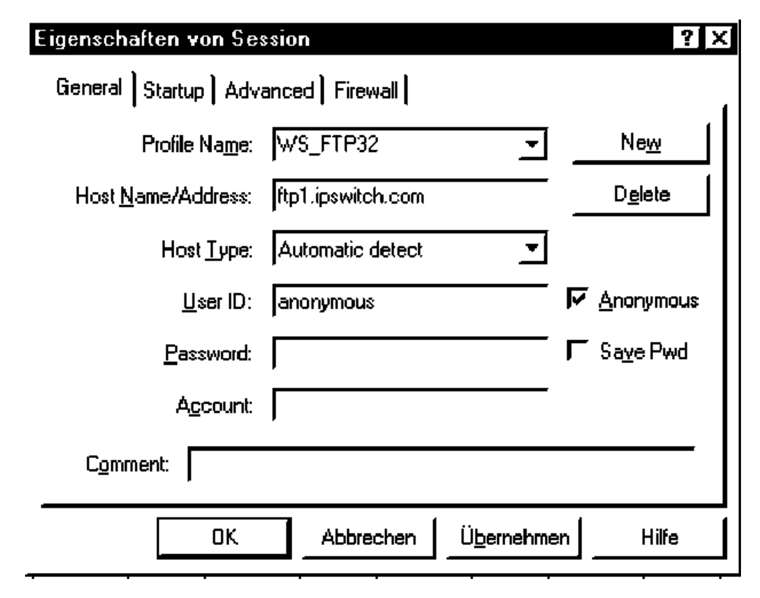



**Abbildung 2-2:** Anmeldung beim \`WS_FTP\`

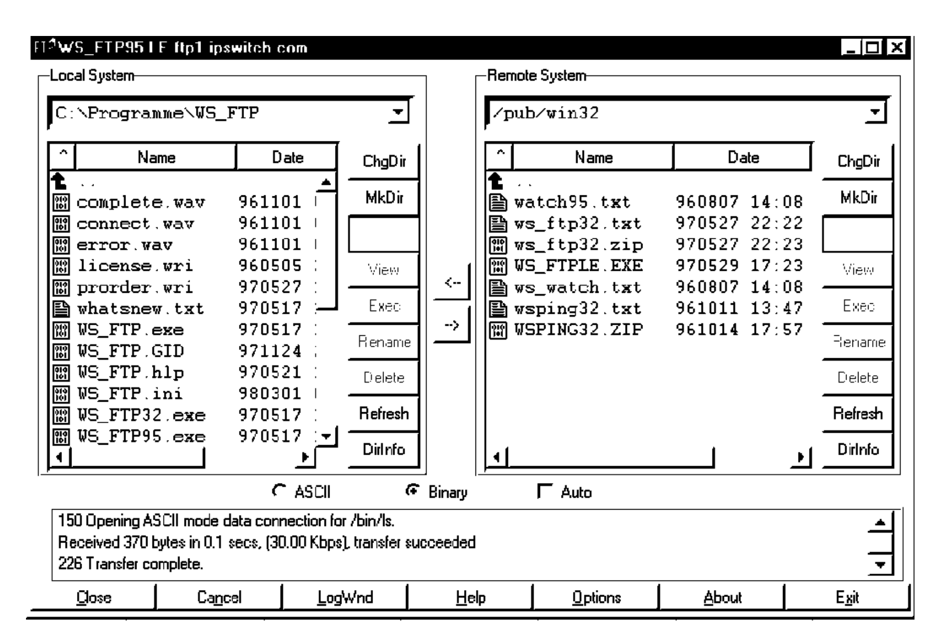



**Abbildung 2-3:** Datenübertragung bei \`WS_FTP\`

### 2.2.4 Sonstige Dienste

#### 2.2.4.1 Newsgroups

In den Newsgroups haben die Internet-Nutzer die Möglichkeit, sich zu informieren oder mit anderen zu diskutieren. In mehr als 10.000 Diskussionsgruppen kann jeder seine Meinung oder seine Fragen veröffentlichen. Diskussionsgruppen können unmoderiert (Inhalte werden völlig frei aufgebaut) oder moderiert (Inhaltskontrolle durch einen Moderator) sein. Die moderierten Diskussionsgruppen weisen erfahrungsgemäß eine höhere inhaltliche Qualität auf. Die Newsgruppen sind auf bestimmten News-Servern organisiert, die nach einem bestimmten Verfahren regelmäßig abgeglichen werden. Eine spezielle Anmeldung zur Benutzung von Newsgruppen ist nicht erforderlich. Jeder kann die Artikel lesen, die ihn interessieren aber auch selbser Texte verfassen.

#### 2.2.4.2 IRC - Inter Relay Chat

Chat ist eine Form der Kommunikation in Echtzeit mittels Tastatur. Dabei kann sich der Benutzer (meist unter einem Pseudonym) bei einem IRC-Server anmelden. Anschließend muss man die Gruppe auswählen, an der man sich beteiligen möchte. Jetzt kann man einen Beitrag mittels Tastatur eingeben. Die anderen angemeldeten Teilnehmer dieser Gruppe bekommen diesen Beitrag nun direkt auf den Bildschirm geschrieben und können entsprechend darauf antworten. Die Beiträge werden üblicherweise in Englisch geschrieben. Zusätzlich schreiben die Chat-Profis mit vielen Abkürzungen und Symbolen, die man sich als Anfänger erst einmal aneignen sollte.

## 2.3 Gefahren

### 2.3.1 Vertrauliche Daten

Aufgrund der Offenheit des Internets und der zalreichen Datenübergänge gibt es viele Möglichkeiten des „Abhörens“ von gesendeten Informationen. Deshalb sollte man persönliche, vertrauliche oder sogar geheime Informationen (z.B. in einer E-Mail) nicht unverschlüsselt über das Internet senden.

Für diesen Zweck gibt es verschiedene Verschlüsselungsprogramme. So gibt es das Programm PGP (pretty good privacy), mit dem E-Mails verschlüsselt versendet werden können. Mit dieser Software werden verschiedene „Schlüssel“ generiert. Der Empfänger einer verschlüsselten Nachricht benötigt dafür allerdings diesen Schlüsselcode zur Dekodierung. Im World Wide Web gibt es mittlerweile viele kostenpflichtige Angebote (Shops etc.). Die Bezahlung erfolgt meist mittels Kreditkarte. Dabei wird man aufgefordert, die

zahlung erfolgt meist mittels Kreditkarte. Dabei wird man aufgefordert, die Kreditkartennummer und die Gültigkeitsdauer einzugeben.

**Diese Daten sollte man niemals unverschlüsselt versenden !**

Die neueren Web-Server und Web-Browser sind in der Lage, Daten in einem Secure-Modus verschlüsselt auszutauschen. Dieser Modus wird auch zum Internet-Banking benötigt.

 **Persönliche oder vertrauliche Daten ausschließlich verschlüsselt versenden !**

## 2.3.2 Computerviren

Computerviren sind kleine Programme, die meistens dafür geschrieben wurden, sich in möglichst kurzer Zeit weit zu verbreiten. So steigern sie den „Ruhm“ ihrs Verfassers. Einige Viren stören die Computer, andere sind darauf ausgelegt Daten zu vernichten oder im Extremfall Hardware zu zerstören.
Auf jeden Fall ist ein „Virenbefall“ gerade in Computernetzen mehr als unangenehm und arbeitsaufwendig. Zur Vermeidung eines Virenbefalls sollten Sie folgende Hinweise beachten:

1. Installieren Sie in Ihrem Netz ein Anti-Virenprogramm, das permanent die Dateien auf Viren prüft und frühzeitig Alarm schlägt.
2. Beschränken Sie den Benutzerzugriff so weit als möglich.
3. Öffnen Sie keine E-Mails mit Anhang unbekannter Herkunft .
4. Sperren Sie ggf. die Diskettenlaufwerke der Workstations.

Viren können über das Internet auf zweierlei Arten verbreitet werden, zum einen durch infizierte Dateien, die Sie z.B. über FTP beziehen. Vermeiden Sie deshalb Datenübertragungen aus unbekannten FTP-Servern. Zum anderen können Viren über Dateien verbreitet werden, die Sie per E-Mail erhalten. Allerdings können sich die Viren nur in Dateianlagen, wie z.B. Word- oder Excel-Dokumenten aufhalten. Reine Textinformationen können keine Viren verbreiten. Oftmals werden Mails weltweit verschickt, in denen steht, dass Ihr PC durch das Lesen eben dieser E-Mail mit einem Virus befallen wird. Diese Mails sind reine Panikmache!

## 2.4 BelWü[1]

BelWü steht für "Baden-Württembergs extended LAN" und ist das Datennetz der wissenschaftlichen Einrichtungen des Landes Baden-Württemberg. Es verbindet zur Zeit über 50.000 Computer von über 80 Teilnehmern miteinander. Das Besondere in diesem Umfeld sind 2 Aspekte: Es werden Hochgeschwindigkeitsverbindungen bis zu 155 MBit/sec (auf der Strecke zwischen Karlsruhe und Stuttgart sowie zwischen Ulm und Stuttgart) genutzt. Weiterhin ist das BelWü das einzige Regionalnetz der Bundesrepublik in der Wissenschaftswelt des DFN, das zentral verwaltet wird.

BelWü wurde als ein über das Land verteiltes Rechenzentrum konzipiert: "BelWü versteht sich als ein ZusammenSchluss der Baden-Württembergischen Hochschulen und Forschungseinrichtungen zur Förderung der nationalen und internationalen Telekooperation und Nutzung entfernt stehender DV-Einrichtungen unter Verwendung schneller Datenkommunikationseinrichtungen. BelWü ist ein organisatorisches Teilnetz im Rahmen des Deutschen Forschungsnetzes. Unbeschadet der innerorganisatorischen Eigenständigkeit der neun Universitätsrechenzentren ist das Kernziel die Darstellung dieser Rechenzentren als eine einheitliche DV-Versorgungseinheit gegenüber den wissenschaftlichen Nutzern und Einrichtungen."[2]

**Management**

BelWü ist derzeit das einzige landesweite Regionalnetz im Hochschulbereich in Deutschland mit einem zentralen Management. Dieses erfolgt durch die BelWü-Koordination in Stuttgart, die beim Rechenzentrum der Universität Stuttgart angesiedelt ist.
Die BelWü-Koordination ist ein Team aus 7 ständigen Mitarbeitern. An jeder der 9 Universitäten des Landes gibt es darüber hinaus jeweils einen weiteren BelWü-Mitarbeiter (BelWü-Beauftragten).

Dies bedeutet, dass
- Funktions- und Leistungsfähigkeit des Netzes ständig überwacht werden
- für das BelWü verantwortliche Ansprechpersonen existieren
- Netzdienste koordiniert und zentral angeboten werden

Über verschiedene Arbeitskreise erfolgt ein stetiger Wissenstransfer zwischen den beteiligten Organisationen. Eine wichtige Funktion haben dabei die BelWü-Arbeitskreise (BelWü-AKs) als regelmäßige Austauschstellen der Netzspezialisten. Dieser enge Kontakt der BelWü-Beauftragten untereinander ist für das Gelingen des BelWü ganz wesentlich, da neben

---

1 Aus: http://www.belwue.de, BelWü-Koordination, Rechenzentrum Universität Stuttgart. April 1997.
2 Aus: Ministerium für Wissenschaft und Kunst Baden-Württemberg: Grundsätze der BelWü-Organisation, 1991, S.1.





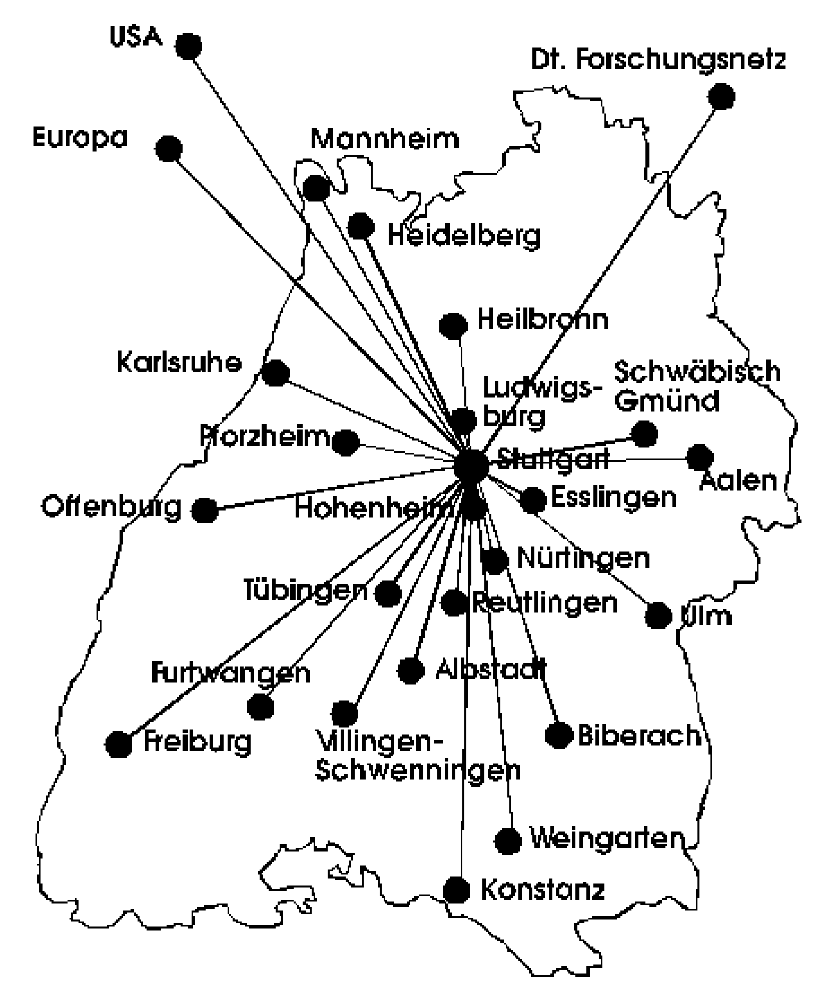
der Lösung von technischen Problemen die konstruktive Zusammenarbeit aller beteiligten Netzfachleute die Qualität ständi verbessert.
Durch die Anwesenheit eines Rechenzentrumsleiters im AK erfolgt die institutionalisierte Verzahnung der relevanten Netzzuständigen.

Es gibt dabei folgende BelWü-Arbeitskreise:

- AK1: Arbeitskreis der Universitäten im BelWü
- AK2: Arbeitskreis der Fachhochschulen, Pädagogischen Hochschulen und Berufsakademien im BelWü
- AK3: Arbeitskreis der Schulen im BelWü

**Topologie**

Das Landesforschungsnetz, das 1987 als reines Universitätsnetz begann und mit Remote Ethernetbridges arbeitete, verbindet heute 79 Einrichtungen mittels Netzverbindungsrechnern (Router).
Für den Datentransfer werden Leitungen mit einer Geschwindigkeit zwischen 64 KBit/sec und 155 MBit/sec verwendet. Ein Beispiel, um die Dimension zu verdeutlichen: die Hochgeschwindigkeitsleitungen ermöglichen die Übertragung eines 20-bändigen Universallexikons in



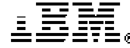



**Abbildung 2-4:** Das BelWü-Netz

weniger als 10 Sekunden. Zwischen Karlsruhe und Stuttgart besteht eine ATM-Strecke mit 155 MBit/s., ebenso zwischen Ulm und Stuttgart. Die Universitäten sind über 34 MBit/s über B-WiN (Breitbandwissenschaftsnetz) voll vermascht. Kleinere Einrichtungen wie Fachhochschulen und Berufsakademien, die sich im Nahbereich von Universitäten befinden, nutzen 2MBit/s - Standleitungen und diejenigen, die noch weiter entfernt leigen, 64 KBit/s-Anschlüsse.

**Nationale und internationale Anbindung:**

Andere bundesdeutsche Netze außerhalb des BelWü werden über B-Win-Anschlüsse mit 34 MBit/s erreicht; der restliche internationale Zugang erfolgt über den DFN mit 45 MBit/s (Europa) und 90 MBit/s (USA), sowie 35 MBit/s zu CERN und SWITCH.

**Weitere Entwicklung von BelWü**

Im Frühjahr 1993 hat der Ministerpräsident des Landes eine Initiative zum Ausbau des BelWü zu einem Hochgeschwindigkeitsnetz initiiert. Nach damaliger Planung sollte bis zum 1.9.97 das ATM-Landeshochschulnetz aufgebaut werden. Die Nutzung des B-Win-Anschlusses beim DFN soll noch bis Dezember 1997 andauern. Mit Beginn des Jahres 1998 sollen dann alle 155-Mbit/s-Strecken zwischen den Universitäten des Landes in Betrieb genommen werden; bisher existiere aber nur eine 155-Mbit/s-ATM-Referenzstrecke zwischen Karlsruhe und Stuttgart sowie eine weitere zwischen Ulm und Stuttgart. Im Juni 1998 sollen dann die Fachhochschulen, Berufsakademien und Pädagogischen Hochschulen im Zusatznetz mit 34 MBit/s angeschlossen sein.
Weitere Infos zu Entwicklungen im BelWü finden Sie auf dem WWW-Server der Abteilung RUS-Kommunikationssysteme und BelWü-Entwicklung.

**BelWü Geschichte**

Einige wichtige Ereignisse in der Geschichte des BelWü sind in der folgenden Liste zusammengefasst.

- 4.Quartal `87 Gründung von BelWü und erste BelWü-Leitung installiert
- 02/88 erste VBN-Strecke eingeweiht, Karlsruhe - Stuttgart
- 05/89 Übergang von einem gebridgten auf ein geroutetes Netz
- 07/89 alle Universitäten an das BelWü angeschlossen
- 11/89 USA-Anschluss
- 02/90 IP über das X.25-Wissenschaftsnetz WIN zu deutschen Internetteilnehmern außerhalb von BelWü
- 04/90 Anschluss der ersten Fachhochschule
- 08/90 SWITCH-Anschluss über Freiburg/Basel
- 02/91 erste Ausgabe der Informationsbroschüre BelWü-Spots
- 09/91 Betriebsmodell der Trennung RZ/BelWü-Router eingeführt
- 02/92 Verbindung zum LVN realisiert (Landesverwaltungsnetz)

- 07/92 In Stuttgart, Heidelberg und Karlsruhe werden Anschlüsse an das neue 2 MBit/s WIN installiert
- 1993 Die BelWü-Koordination gewinnt die Ausschreibung "IP-Management für Deutschland" des DFN-Vereins
- 01/94 Anschluss der ersten Schule
- 07/94 Vollvermaschung der Universitäten über Datex-M (2-34 MBit/s)
- 09/94 BelWü bietet Verbindungen zwischen neun Universitäten, 20 Fachhochschulen und sieben Berufsakademien an
- Baden-Württemberg und weitere 18 Einrichtungen haben mehr als 25000 Rechnern.

### 2.4.1 Übersicht

BelWue - Netscape

Datei Bearbeiten Ansicht Gehe Communicator Hilfe

Zurück Vor Neu laden Anfang Suchen Guide Drucken Sicherheit Stop

Lesezeichen Adresse: http://www.belwue.de/

Baden-Württembergs extended LAN

BelWü

Das Hochschulnetz in Baden-Württemberg

Willkommen beim WWW-Service des BelWü!

Hier finden Sie Allgemeines zu BelWü aber auch aktuelle Netzwerkmanagement-Daten.

Haben Sie noch Fragen an uns oder vielleicht Infos für uns? Hier ist unsere Adresse, Sie können aber auch direkt aus dem WWW eine Nachricht an uns schicken.

**Aus der Arbeit des BelWü**

- Was ist BelWü?
- Netztopologie und Netzmanagement
- BelWü-Arbeitsgruppen
- BelWü-Entwicklung

**Dienste und Angebote**

- BelWü-Services
- Virtuelle WWW-Server auf www.belwue.de
- Modem-Einwahl über Hochschulen im BelWü

Dokument: Übermittelt

**Abbildung 2-5:** Startseite des Baden-Württembergs extended LAN unter http://www.belwue.de

### 2.4.2 Warum das BelWü für Schulen ?

Das BelWü versteht sich, wie bereits in 2.4 dargestellt, als ein ZusammenSchluss von Baden-Württembergischen Hochschulen und Forschungseinrichtungen und ist allein schon aus diesem Grund prädestiniert für Schulen. Der Anschluss ans Internet über BelWü ist für Schulen zunächst **kostenlos**, geplant sind in Zukunft monatliche Gebühren von DM 30,-. Zum Vergleich: Andere Provider verlangen für vergleichbare Leistungen ca. 3000,- bis 5000,- DM.

Lediglich für die Verwendung eines CISCO-Routers, den Sie vorkonfiguriert von BelWü erhalten, entstehen monatliche Gebühren von 50,- bzw. 60,- DM (abhängig vom Typ des Routers). Dieser Router ist das Bindeglied zwischen Ihrem lokalen Netz und dem Provider BelWü. Sie können alternativ einen eigenen Router verwenden oder den Router von BelWü käuflich erwerben (1680,- DM bzw. 2500,-). Im Leistungsumfang des Internet-Anschlusses sind ein E-Mailservice (Zustellung von E-Mail aus dem Internet und ins Internet) sowie für jede Schule ein eigener virtueller Web-Server enthalten, auf dem Sie Webseiten Ihrer Schule ablegen und im Internet veröffentlichen können. Ferner bietet BelWü für jede Schule Unterstützung bei der Beschaffung und Verwendung der empfohlenen Hardware an. Insbesondere können Ihnen – sofern Ihre lokalen Voraussetzungen dies erfordern - in Rücksprache mit BelWü für Ihr lokales Netz beliebig viele IP-Adressen zur Verfügung gestellt werden. Für technische Details sei an dieser Stelle auf das nächste Kapitel verwiesen.

### 2.4.3 Anbindung Ihres Schulnetzes an BelWü[3]

BelWü, das Landesforschungsnetz Baden-Württembergs, wird finanziert vom Ministerium für Wissenschaft, Forschung und Kunst (MWK) und betrieben von der BelWü-Koordination am Rechenzentrum der Universität Stuttgart (RUS) in Zusammenarbeit mit den jeweiligen lokalen Rechenzentren der BelWü-Teilnehmer. Im Rahmen von BelWü werden insbesondere wissenschaftliche Einrichtungen (die 9 Landesuniversitäten, über 20 Fachhochschulen, die acht Berufsakademien, etc.) über schnelle Datenleitungen untereinander verbunden. Zwischen den Universitäten existieren 155 MBit/s Verbindungen, die Fachhochschulen sind i.d.R. mit 2 oder 34 MBit/s angebunden, kleinere Einrichtungen teilweise noch mit 64 KBit/s Festverbindungen.

Schulen können sich an 155, 34 oder 2 MBit/s BelWü Aufpunkte mittels 64 KBit/s ISDN-Wähl- oder Festverbindungen anschließen. Wenn ein 64 KBit/s BelWü-Teilnehmer im Nahbereich liegt, kann dies evtl. mit dem expliziten Einverständnis des betreffenden Aufpunktes erfolgen. Aufpunkte mit 2 MBit/s oder größer sind derzeit: Aalen, Albstadt, Biberach, Freiburg, Furtwangen, Göppingen, Heidelberg, Heilbronn, Karlsruhe, Konstanz, Künzelsau, Lörrach, Ludwigsburg, Mannheim, Mosbach, Nürtingen, Offenburg, Pforzheim, Reutlingen, Rottenburg, Schwäbisch Gmünd, Stuttgart, Tettnang, Trossingen, Tübingen, Ulm, Villingen-Schwenningen, Walldorf und Weingarten. Eine Leitungserhöhung ist geplant für Heidenheim und Horb. Weitere Zugänge werden bei entsprechender Nachfrage geschaltet; derzeit sind Baden-Baden, Bad-Mergentheim, Calw, Crailsheim, Freudenstadt und Waldshut-Tiengen geplant.

Als Technik wird bei der Schule ein spezieller Netzverbindungsrechner (Cisco-Router) eingesetzt, der einerseits an einen ISDN-Hauptanschluss und andererseits mittels Twisted Pair Ethernet (10BaseT) an das lokale Netz (LAN) der Schule angeschlossen wird (eine Umsetzung von Thinwire Ethernet/10Base2/RG58/BNC auf den 10BaseT-Anschluss des Cisco-Routers erfolgt ggf. über einen MiniHub oder AUI/BNC-Transceiver). Hierdurch wird an der Schule kein PC mit ISDN-Karte benötigt. Beim nächstgelegenen BelWü-Aufpunkt steht eben-

[3] Überwiegend aus: http://www.belwue.de, BelWü-Koordination, Rechenzentrum Universität Stuttgart. Januar 1998.

falls ein entsprechender Cisco-Router. Durch diese Technik kann die Verbindung auch im Fehlerfall von der BelWü-Koordination in Stuttgart betreut werden - ohne manuelle Eingriffe vor Ort.

Für Schulen, die die Kosten für den Cisco-Router nicht tragen können (insbesondere bei Einzelplatzanschlüssen), besteht die Möglichkeit, sich mittels schuleigener ISDN Soft- und Hardware an den BelWü-Aufpunkt aufzuschalten. Hierfür kann bei der Installation, dem Betrieb und der Fehlersuche keine Unterstützung von Seiten der BelWü-Koordination erfolgen. Es gibt jedoch einem Test, der die korrekte Installation überprüft:, wenn Sie den BelWü-Aufpunkt per ISDN erreichen, haben Sie richtig konfiguriert. (Als Hinweis für diesen Weg: der BelWü-Aufpunkt ist mit PPP ohne CHAP und ohne PAP, aber mit CLI konfiguriert).

Im LAN der Schule sind per Ethernet die dortigen Rechner untereinander und über die ISDN-Wählverbindung mit dem gesamten Internet verbunden. Im LAN können sich ein PC, aber auch mehrere Hundert davon befinden. Die Internetadressen für die PCs stammen entweder aus dem Bereich der BelWü-Koordination oder, wenn möglich, aus dem Bereich des lokalen BelWü-Aufpunkts. Diese Adressen sind nur für den Anschluss über das BelWü zu verwenden und können sich auch ändern, wenn der Zugang über einen anderen BelWü-Aufpunkt erfolgt.

Bezüglich des DNS-Namens findt man die Rechner der Schule unter dem Begriff: <Schulkürzel>.<KFZ-Kennzeichen>.bw.schule.de, z.B. pc1.fes.es.bw.schule.de. Als erster Rechnername wird "server" verwendet - dort laufen potentiell Internetdienste wie Mail oder News (server.fes.es.bw.schule.de). Die Abbildung von Internetadresse zu Rechnername (Name-Server) erfolgt auf einem Rechner (Name-Server) der BelWü-Koordination. Was eine Mail betrifft, so werden die Schulrechner von einem Mailrelay der BelWü-Koordination versorgt, der die Post für die Schule eine gewisse Zeit zwischenspeichert (z.B. 14 Tage) und dann an den schuleigenen Mailbox-Server weiterleitet. Der Betrieb eines eigenen Mailboxservers an der Schule wird vorausgesetzt (z.B. unter Novell, Windows NT oder Linux). In Ausnahmefällen (z.B. Einzelplatzanschluss) ist eine Pop-Mailbox für die gesamte Schule möglich - hier muss der Lehrer die Mails an die verschiedenen Empfänger von Hand weiterverteilen. Die Schule erhält Speicherplatz auf einem FTP- bzw. WWW-Server der BelWü-Koordination, wo entsprechende Daten bzw. Seiten der Schulen abgelegt werden können.

Hierfür wird als Rechnername FTP.- bzw. www.<Schulkürzel>.<KFZ-Kennzeichen>.bw.schule.de verwendet, z.B. FTP.fes.es.bw.schule.de bzw. www.fes.es.bw.schule.de.

Hinsichtlich des Gebrauchs von WWW wird der Einsatz eines Proxy-WWW-Servers an der Schule empfohlen, um die geringe Bandbreite von 64 KBit/s optimal zu nutzen. News können von News-Servern der BelWü-Teilnehmer gelesen werden bzw. es kann bei Bedarf eine Untermenge von der BelWü-Koordination bezogen werden.

Musterlösungen obiger Internetanwendungen sollen für die verschiedenen Betriebsysteme der Schulen von der ZPG des LEU Stuttgart erarbeitet werden. Das LEU steht in der Vorphase des Anschlusses der Schule beratend zur Verfügung.

Für den Zugang per Modem empfehlen wir das WiN-Shuttle Projekt.

Siehe hierzu http://www.shuttle.de oder 030/884299-0 (DFN-Geschäftsstelle).

## Kosten

Für den Zugang über das BelWü wird derzeit **keine Gebühr** erhoben. Trotzdem fallen folgende Kosten pro Monat an:

- **Wählverbindungsgebühren** bei der Schule

- ggf. **Router** an der Schule:

  - **DM 50.-/Monat** oder 1680.- einmalig: **Cisco mit 1 Ethernet und 1 ISDN** (Cisco1003 oder Cisco1603)

  *oder*

  - **DM 60.-/Monat** oder 2500.- einmalig: **Cisco mit 2 Ethernet und 1 ISDN** (Cisco1605 mit ISDN-Karte), z.B. zur Trennung von Schul- und Verwaltungsnetz

  Der Router bleibt bei der Beschaffung über das BelWü im Eigentum der Universität Stuttgart, d.h. Wartung oder Ersatz bei Defekt gehen nicht zu Lasten der Schule.

Alternativ zur Wählverbindung kann eine ISDN-Festverbindung gewählt werden. Dies ist vor allem attraktiv, wenn Hochschule und Schule am selben Ortsvermittlungsknoten der Telekom angeschlossen sind (Auskunft gibt die Telekom):

- Telekomgebühr: DM 250.-/Monatspauschale plus einmalige Installationsgebühren für DM 4000.- für 128 KBit/s (DS02)
- BelWü-Gebühr: DM 50.-/Monat oder 1680.- einmalig für Router am Aufpunkt

## Antragstellung

Bei Interesse an einem Anschluss füllen Sie bitte das **Online-Formular** aus, das Sie unter

http://nic2.belwue.de/anschluss/schulform.html

im Internet finden. Dieses Formular enthält detaillierte Informationen über alle Angaben, die BelWü zur Bearbeitung Ihres Antrags benötigt.

Sollten Sie keinerlei Zugang zum Internet haben, genügt auch ein formloser Brief an die BelWü-Koordination, Rechenzentrum der Universität Stuttgart, Allmandring 30, 70550 Stuttgart. Ansprechpartner ist hierfür z.Zt. Peter Merdian, schul-anschluss@belwue.de, Tel. 0711/685-5804, Fax 0711/6787626. Zusätzlich sollen im letzteren Fall per E-Mail (falls möglich - jedoch nicht als Mail-Attachment oder Word-Dokument -, ansonsten per Gelber Post) die im Anhang aufgeführten technischen Einzelheiten angegeben werden.

Daraufhin wird sich die BelWü-Koordination mit den in Frage kommenden BelWü-Aufpunkten in Verbindung setzen, um dort eine im Nahbereich liegende Anbindung zu ermöglichen.

Zum Schluss ein Haftungshinweis:

1. Wie aus der Presse und anderen Medien allseits bekannt, ermöglicht das Internet Zugriff auf Informationen, die gegen deutsche Gesetze verstoßen (Rassismus, Radikalismus, Pornographie usw.). Es ist dem BelWü unmöglich, den Zugang zu diesen Informationen zu unterbinden. Während man bei den Mitgliedern der wissenschaftlichen Einrichtungen, die das Internet nutzen, davon ausgehen kann, dass sie volljährig sind, ist dies bei Schülern in der Regel nicht der Fall. Aus dieser Tatsache könnten sich weitere juristische Probleme ergeben. Das BelWü kann daher keine Haftung für den Inhalt der über das Netz transportierten Informationen übernehmen.
2. Bei der Benutzung der Netzwerkdienste ist auf die Einhaltung der deutschen Gesetze zu achten. Dies betrifft vor allem das Verschicken von unverlangter Werbung ("Spams") und von Dateien mit illegalem Inhalt. Bei Zuwiderhandlung behält sich die BelWü-Koordination vor, die entsprechenden Artikel zu Löschen oder bei strafrechtlich relevantem Inhalt die Staatsanwaltschaft einzuschalten, sowie bei wiederholtem Mißbrauch den Netzzugang des Teilnehmers zu sperren.
3. Für den Inhalt von WWW-Seiten des Teilnehmers auf einem BelWü-Server ist der Teilnehmer selbst verantwortlich.

============== **Anhang: Anschlussinformationen** (Antrag) ====================

Im Antrag sind insbesondere folgende technische Daten von Belang:

1. ISDN Rufnummer mit Angabe des Typs (Euro oder nationales ISDN). Ggf. Hinweis, wenn beim Wählen nach Außen eine zusätzliche "0" notwendig ist. Bitte beachten Sie, dass bei Euro-Anschlüssen die erste der drei möglichen Rufnummern (MSN) genommen wird. Geben Sie an, nach wieviel Sekunden Verbindungszeit eines Monats automatisch eine Mail zur Warnung an die technischen Kontaktpersonen verschickt werden soll. Ggf. Termin, wann der ISDN-Anschluss bereit steht bzw. bis wann der Anschluss geplant ist. Ggf. Hinweis, ob bei Einsatz eines Cisco-Routers an der Schule die Verbindung aufgrund eines Telekom-Gebührenimpulses taktgenau bei Übertragungspausen abgebaut werden soll. Der hierfür notwendige Telekomdienst heißt AOC-D und kostet zusätzlich 1,30 DM/Monat zzgl. MWSt. pro B-Kanal an die Telekom.

2. Anzahl der Rechner mit Angabe des Betriebssystems; hier nur Rechner angeben, die eine eigene IP-Adresse benötigen (dies ist ggf. in einem Novellnetz relevant, in dem nur der Server direkt im Internet sein soll). Wenn mehrere Ethernetnetze über einen Server verbunden sind, wird die genaue Topologie (v.a. Angabe der Rechneranzahl pro Strang) benötigt. Für die Adreßvergabe ist noch interessant, wie sich die Rechneranzahl in den nächsten 1 bzw. 2 Jahren entwickeln wird.

3. Da der Cisco-Router lediglich einen 10BaseT-Ethernet Port (RJ45) besitzt, muss angegeben werden, wenn im LAN kein Port verfügbar ist (z.B. wenn im LAN nur 10Base2 Ethernet/RG58/BNC-Verkabelung eingesetzt wird).

4. Rechnernamen für jeden Rechner, der eine eigene IP-Adresse benötigt. Im Beispiel unten heißen die Rechner (außer dem Server) rechner01, rechner02, etc. Bitte tragen Sie hier Ihre eigenen kurzen Rechnernamen ein. Zusammen mit dem Domainzusatz ergibt sich dadurch der weltweit eindeutige Rechnername (z.B. server.fes.es.bw.schule.de).

5. Hochschulstadt, die sich im selben Telefon-Ortsbereich befindet zwecks kostengünstigem Anschluss.

6. Hinweis, ob mit dem potentiellen nicht-universitären BelWü-Aufpunkt bereits über die Installation eines ISDN-Haupanschlusses am dortigen Rechenzentrum gesprochen wurde.

7. Vom StandardAnschluss abweichende Punkte, wie Einsatz keines Cisco-Routers bzw. Einsatz einer Popmailbox anstelle eines Mailboxservers.

Nachfolgend finden Sie ein **ausgefülltes Musterformular**, das sie im Internet unter

http://www.belwue.de/BelWue/schul-anschluss.html#Antragsformular

finden. Es soll an dieser Stelle nur als Beispiel dienen, um aufzuzeigen, welche Informationen in welcher Form benötigt werden. Wenn Sie, wie oben erwähnt, das **Online-Formular** ausfüllen, bekommen Sie zu jedem einzelnen Punkt eine detaillierte Hilfestellung. Das **Online-Formular** finden Sie unter

http://nic2.belwue.de/anschluss/schulform.html

Sie sollten daher, wenn möglich, unbedingt letztere Form der Antragstellung wählen.

```
*de: Franz-Erich-Schule Esslingen
*rm: Berufschule, Techn. Gymnasium, Technikerschule, 1200 Schueler, 80 Lehrer
*kn: FE-Schule-Esslingen
*or: 29999
*ad: Hauptstr. 111, 73730 Esslingen-Zell. Tel: 0711/9999-0, Fax: -666
*rm:
*ac: Maria Musterfrau,  0711/9999-111,
*tc: Thomas Mustermann, 0711/9999-222, 123456.789@compuserve.com
*tc: Wolfgang Kollege,  0711/9999-333, Wolfgang.Kollege@t-online.de
*rm:
*rm: ----- Anschluss -----
*in:
*rm: 50 PCs mit Windows95, an zwei Ethernetstraengen (Strang1: 20, Strang2: 29,
*rm:                                  plus 1 Server als Vermittlungsknoten)
*rm: in 1 Jahr ca. 50 Rechner, in 2 Jahren ca. 70 Rechner.
*la:
*co: 64 Euro-ISDN-Waehlverbindung+0 0711/9301111 10000
*sy: Cisco-Router ueber Monatsgebuehr finanziert gewuenscht
*rm: 10BaseT-Ethernet Port im LAN nicht vorhanden
*rm: Im Telefon-Ortsbereich von Esslingen und Stuttgart
*rm: *bb: uniXX,Waehl
*rm: *st: xx.xx.97 connected
*rm:
*rm: ---- Name-Server (Domain, Primary, Secondary NS), Mailhost, WWW, Spots ----
*dn: fes.es.bw.schule.de gewuenscht
*rm: Strang1:
*rm: server    = 129.143.xxx.xx
*rm: rechner01 = 129.143.xxx.xx
*rm: rechner20 = 129.143.xxx.xx
*rm: Strang2:
*rm: server    = 129.143.xxx.xx
*rm: rechner21 = 129.143.xxx.xx
*rm: rechner49 = 129.143.xxx.xx
*rm:
*rm: ----- Mail -----
*mx: noc.belwue.de, 14 Tage Verweildauer der Post in der Warteschlange gewuenscht
*mb: server.fes.es.bw.schule.de (129.143.xxx.xx, Pentium PC, Linux, POP-SW)
*rm:
*rm: ----- WWW-Server -----
*ww: http://www.fes.es.bw.schule.de/ auf nic.belwue.de gewuenscht
*rm:
*rm: ----- BelWue Spots -----
*bs: 3 Spots
*rm:
*rm: ----- Rechnungen -----
*rm:
*fc: Maria Musterfrau, Franz-Erich-Schule, Hauptstr. 111, 73730 Esslingen-Zell
*re:
*rm:*rm: ----- Sonstiges -----
*rm: 17.03.97 Antrag auf BelWue-Anschluss. Gewuenschter Anschlusstermin ist
*rm:          der 1.4.97.                                          (Mustermann)
*rm:
*rm: Antrag | BW-Router | K-Router |Ltg.|DNS|Mail|WWW| Offene Fragen
*s1: 970317 | konfig    |          |    |   |    |   |
*rm:
*rm: ***************************************************************************

Die relevanten Kürzel lauten:

*rm: Remark (es ist wichtig, dass der Eintrag einer Organisation nicht durch
*rm:         Leerzeilen unterbrochen wird; also *rm: bei Leerzeilen eintragen).
*de: Description (lange Bezeichnung)
*kn: Kurzname    (kurze Bezeichnung fuer BelWue-interne Zwecke)
*or: Ordnungsnummer (wird von der BelWue Koordination vergeben, Default: 29999)
*ad: Adresse  (Strasse, Postleitzahl, Ort, Telefonzentrale, Fax) in einer Zeile
*ac: Administr. Kontakt (Name, Telefon, Mailadresse, Funktion) in einer Zeile
*tc: Techn.     Kontakt (Name, Telefon, Mailadresse, Funktion) in einer Zeile
*rm:            Diese Mailadresse wird in die BelWue-AK3 Mailliste aufgenommen
*in: Netz       (Rechneranzahl, Betriebssyteme)
*la: IP-Adresse des Anschlusses (Link Adress, von der BelWue Koord. vergeben)
*co: Connect (Bandbreite, Anschlussart: ISDN-Waehlverbindung, ISDN-FV-DS02)
*rm:   Z.B. *co: 64 Euro-ISDN-Waehlverbindung+0 0711/1234    (bei Amts-"0")
*rm:   oder *co: 64 1TR6-ISDN-Waehlverbindung   0711/1234    (ohne Amts-"0")
*rm:   oder *co: 64 1TR6-ISDN-Waehlverbindung 0711/1234 9999 (max. 9999 Sek/Monat)
*sy: System des Netzzugangsknoten (Typ, ggf. Finanzierung)
*dn: Domainname der Schule
*mx: Mailrelay (Domainname, IP-Adresse, Betriebsystem)
*mb: Mailboxserver (Domainname, IP-Adresse, Betriebsystem, Mailsoftware)
*bs: BelWue-Nutzerzeitschrift (gewuenschte Anzahl)
*fc: Finanzieller Kontakt (Rechnungsanschrift) in einer Zeile
*re: Rechnungsinformationen
```

# 3 Linux

## 3.1 Was ist Linux?

Anfang 1991 fing der finnländische Student Linus Torvalds damit an, die Möglichkeiten seines neuen Intel-386-Prozessors in seinem neuen PC zu studieren. Nur ein halbes Jahr später hatte er ein kleines, lauffähiges Betriebssystem programmiert, welches er per E-Mail an interessierte Systemprogrammierer in aller Welt schickte. Torvalds bot seine eigene Entwicklung von Anfang an frei an. Jeder konnte die Quelltexte bekommen und daran mitarbeiten. Bereits im Januar 1992 wurde ein stabil laufender Kernel[4] herausgegeben. Dieses Betriebssystem wurde per anonymous FTP weltweit verteilt. Die Anzahl der weltweit verteilten Programmierer, Tester und Unterstützer wuchs so schnell, dass die Kommunikation per E-Mail nicht mehr ausreichte und somit im USENET eine Rubrik zum Thema LINUX eingerichtet wurde. Dieses Medium und der anonyme FTP-Service im Internet ermöglichten eine Programmentwicklung, wie sie sich große Softwarehäuser nur erträumen konnten. Innerhalb weniger Monate entstand ein ausgewachsenes Betriebssystem mit vollständiger UNIX-Funktionalität.

Auch heute ist Linux im Gegensatz zu kommerziellen Betriebssystemen wie Microsoft® DOS oder Microsoft® Windows 95 eine Freeware und somit kostenlos erhältlich. Man benötigt nur die richtige Internet-Adresse und kann sich dort die aktuellste Version herunterladen. Seit Linus Torvalds vor einigen Jahren seine Arbeiten an einem UNIX-ähnlichen Betriebssystemkern für Intel-basierte PCs begann, hat sich viel getan. Linux hat sich vom „Hackerspielzeug“ zu einem ausgereiften Betriebssystem entwickelt, dessen Leistungsmerkmale den Vergleich mit anderen, wesentlich älteren (und mittlerweile schwerfälligeren) Systemen nicht zu scheuen braucht.

Die Verwendung von **UNIX** war lange Zeit den Besitzern und Nutzern teuerer Hochleistungsrechner vorbehalten. Dieser Eindruck verstärkt sich noch durch einen enormen Schulungsaufwand für die von der Umstellung betroffenen Mitarbeiter. Mit Linux eröffnet sich für die PC-Welt die Gelegenheit, zu einem vernünftigen Preis ein multi-user/multi-tasking[5]-Betriebssystem kennenzulernen. Eine wachsende Zahl von Anwendern wird erst über Linux die Welt der UNIX-ähnlichen Systeme betreten.

---

[4] Der Begriff "Betriebssystem" wird für zwei verschiedenen Bedeutungen benutzt. Das Betriebssystem im engeren Sinne wird auch als Kernel verstanden. Die komplette Installation eines Basissystems mit Kernel, Dateisystem, Shell und Utilities wird oft auch als Betriebssystem bezeichnet.

[5] „Multi-user“: Mehrere Benutzer können gleichzeitig am selben System angemeldet sein und auf voneinander unabhängigen Konsolen arbeiten. „Multi-tasking“: Es können gleichzeitig verschiedene Prozesse (Programme) laufen.

Ein komplettes Linux-System ist bereits für weniger als 100 DM [6] erhältlich und wenn nicht gerade in einem kommerziellen Umfeld Linux als kostengünstige Alternative zu sogenannten „proprietären UNIXen“ gewählt wird, stehen die Aufwendungen für eine Schulung dazu in keinem Verhältnis. Außerdem wenden sich immer mehr PC-Besitzer aus rein privaten Interesse der „Faszination Linux“ zu. Auch für den kommerziellen Einsatz von Linux sprechen viele Argumente: Durch den freien Status von Linux kann eine große Zahl von Rechnern mit einem leistungsfähigen System ausgestattet werden, ohne dass hohe Lizenzgebühren anfallen.

Das schlagkräftigste Argument für Linux überhaupt dürfte jedoch die Verfügbarkeit des kompletten Quellentextes sein. Neben der Möglichkeit, das System nach Belieben an die eigenen Bedürfnisse anzupassen, muss bei der Suche nach schwierigen Fehlern nicht beim Betriebssystem halt gemacht werden. Das resignierte „Damit müssen wir halt leben“, das man von herkömmlichen Systemen gewohnt ist, kann somit einem „Das werden wir halt ändern“ weichen; diese Dynamik und Einflussnahme auf das Betriebssystem ermöglicht erst die rasante Entwicklung und beeindruckende Stabilität von Linux.

Daneben ist Linux äußerst kooperativ. Es lässt sich völlig problemlos mit beliebigen anderen Systemen auf demselben Rechner installieren und bietet vielfältige Möglichkeiten der Kommunikation und des Datenaustausches mit diesen Systemen.

In neuerer Zeit erhält Linux vermehrt Zuspruch aus dem Lager der Nur-Anwender. Diesen Durchbruch schaffte Linux nicht zuletzt durch die Verfügbarkeit hochwertiger Applikationen, wie Office-Paketen (Applix*ware*, StarOffice), Datenbanken (Adabas D) oder viele andere Anwendungen im professionellen und wissenschaftlichen Bereich. Komplettiert wird das ganze durch die grafische Benutzeroberfläche Xfree86 (derzeit Version 3.3), ein X-Window-System für PC-basierte UNIX-Systeme. Alle diese Komponenten, zusammen mit zusätzlichen Tools und Goodies (wie z.B. Spiele), bilden das System, das gemeinhin als *Linux* bezeichnet wird.

Wie bereits erwähnt, existiert für UNIX jedoch ein geradezu unerschöpfliches Reservoir an freier Software, so dass es praktisch beliebig viele Möglichkeiten gibt, ein Linux-System zusammenzustellen.

## 3.2 Distributionen

Dadurch, dass Linux als sog. Freeware aus vielen Teilen besteht, die von unterschiedlichen Programmierern in der ganzen Welt unabhängig voneinander entwickelt wurden, gibt es kein "offizielles" Linux-Installationspaket, in dem alle verfügbare Programme zusammengefasst sind. Mehrere Gruppen und Unternehmen bieten jedoch mittlerweile den Linux-Kernel zu-

[6] Man bezahlt für die „Distribution“, nicht für Linux selbst!

sammen mit vielen Utilities, Applikationen und Installationsprogrammen in einem Paket an. Dieses Paket wird auch als Distribution bezeichnet, welche gegen eine Gebühr (ca. 60 - 150 DM) vertrieben wird. Daneben sind die meisten Distributionen auch im Internet frei abrufbar, so dass gelegentliche Updates des Systems nicht den Neukauf einer Distribution bedingen.

Allerdings müssen die Benutzer dazu das mehrere hundert Megabyte große Betriebssystem aus dem Internet herunterladen und von Hand installieren. Dies erfordert einige UNIX-Kenntnisse und viel Geduld. Im Gegensatz dazu sind auf den meist per CD vertriebenen Distributionen einfach zu bedienende Installationsprogramme enthalten. Zusätzlich erhält der Käufer auch ein Handbuch.

Die Distributoren sichten das Riesenangebot an frei erhältlicher und frei vertreibbarer Software und treffen eine Auswahl. Das Ergebnis dieser Auswahl ist im Falle der S.u.S.E. Linux-CDs, welche in diesem Kurs behandelt wird, eine Zusammenstellung von ca. 600 Softwarepaketen.

Es existiert mittlerweile ein regelrechter Dschungel von Linux-Distributionen und Versionen. Die in Deutschland am häufigsten verbreitete Linux-Distribution ist das S.u.S.E.-Linux. Darüber hinaus gibt es z.B. noch die Slackware- (in englisch) oder die DLD-Distribution (in deutsch).

## 3.3 Linux-Bezugsquellen

Da der Bekanntheitsgrad von Linux in letzter Zeit stark angestiegen ist, gibt es mittlerweile viele Möglichkeiten, die o.a. Pakete und zusätzliche Programme aus dem Internet herunterzuladen. Der direkteste und somit schnellste Weg, einzelne Programme und Kernel-Versionen zu beziehen, ist der Zugriff auf einen FTP-Server. Der wichtigste Linux-FTP-Server in Europa ist **nic.funet.fi** in Finnland, der auch der erste Linux-Server überhaupt war. Auf ihm finden sich die neuesten Kernel-Versionen. Ein breites Angebot an Linux-Software findet sich bei **sunsite.unc.edu** in den USA. Damit das Internet nicht unnötig belastet wird und da die Verbindung zu einem deutschen Server meistens schneller ist, werden diese Linux-Server auf deutsche FTP-Server gespiegelt. D.h., dass die Dateien der FTP-Server in den USA in regelmäßigen Abständen auf die deutschen FTP-Server kopiert werden. Einige dieser sog. Mirror-Server sind:

- FTP.informatik.hu-berlin.de
- FTP.uni-erlangen.de
- FTP.germany.eu.net
- FTP.rz.uni-karlsruhe.de
- FTP.rz.uni-ulm.de

## 3.4 Linux-Informationsquellen

Im Lieferumfang der S.u.S.E.-Distribution sind eine Vielzahl von Dokumentationen und Informationen zu Linux enthalten, das meiste davon allerdings in englisch. Nach der Installation der Paketserie **doc** sind im Verzeichnis `/usr/doc` folgende Unterverzeichnisse zu finden:

| | |
|---|---|
| `/faq` | Frequently asked questions, die am meisten gestellten Fragen mit entsprechenden Antworten (in englisch) |
| `/howto` | Detailbeschreibungen bestimmter Aspekte der Konfiguration oder Anwendung von Linux (in englisch) |
| `/packages` | Ausführliche Informationen zu den installierten Paketen (z.B. PPP) (in englisch, teilweise in deutsch) |
| `/susehilf` | Das Hilfesystem von S.u.S.E.-Linux als Html-Dateien (in deutsch und englisch) |
| `/wie_geht` | Howto (s.o.) in deutsch |

Zusätzlich gibt es im Internet eine Vielzahl von Newsgroups zum Thema Linux, sowohl in Deutsch als auch in Englisch (bspw. de.comp.os.linux.misc).

# 4 TCP/IP-Grundlagen

## 4.1 Überblick

Netzwerke sind wahrscheinlich so alt, wie die Kommunikation der Menschen untereinander. Stellen Sie sich die Steinzeitmenschen vor, die Trommeln zum Austauschen von Nachrichten benutzt haben. Fred Feuerstein möchte Barnie Geröllheimer zum Dinosaurier-Jagen einladen. Allerdings wohnt Barnie so weit von Fred entfernt, dass dessen Trommel zur Verständigung nicht ausreicht. Fred kann also 1. zu Barnie hingehen und ihn direkt informieren, 2. sich eine größere Trommel besorgen oder 3. Wilma bitten, die genau zwischen Fred und Barnie wohnt, die Nachricht weiterzuleiten. Letzteres wird als ein Netzwerk bezeichnet.

Heute sind Computer, eine Möglichkeit zur Kommunikation, über Kabel oder Glasfaserverbindungen vernetzt. Ein Netzwerk besteht aus verschiedenen Computern, die miteinander kommunizieren können. Kommunikation ist nur auf einer gemeinsamen Ebene möglich, z.B. einer Sprache. In Computernetzwerken wird die Sprache als Protokoll bezeichnet. Bei Protokollen sollten Sie allerdings nicht an geschriebene Protokolle, sondern vielmehr an das sehr strenge Protokoll bei einem Staatsempfang denken. Denn ähnlich wie beim Protokoll eines Staatsempfangs legen Computerprotokolle auf eine sehr formalisierte Art und Weise strenge Regeln für den Nachrichtenaustausch zwischen mehreren Computern fest. Ein sehr weit verbreitetes Protokoll ist das im Unix-Bereich obligatorische TCP/IP-Protokoll. Dabei werden die Daten in kleine Einheiten, sog. Pakete, zerlegt und direkt an den Zielrechner weitergeleitet. Der Zielrechner setzt diese kleinen Pakete wieder zusammen und verarbeitet die Informationen weiter. Ein solches Verfahren wird auch als paketorientiertes Netzwerk (im Englischen *paket-switched*) bezeichnet.

## 4.2 Internet-Protokoll (IP)

Das Internetprotkoll ist für die Adressierung im Netzwerk zuständig. Daher werden wir uns intensiver mit der Adressierung von Netzwerken, insbesondere der IP Adressierung beschäftigen.
Die Struktur der IP Adressierung hat folgenden Aufbau

Eine IP Adresse wird durch vier binäre Zahlen, die durch Punkte getrennt sind, dargestellt. Die binäre Darstellung einer dezimalen Zahl der IP Adresse besteht aus acht Stellen. Somit sind die Zahlen 00000000 bis 11111111 möglich. Da die binäre Zahl acht Stellen hat, sind $2^8$ Zahlen möglich. Dies sind 256 Zahlen. Die Null wird als Zahl gewertet, so dass die größte

Zahl 255 ist. Eine typische IP Adresse lautet 125.30.5.200. In der binären Ansicht entspricht diese IP Adresse 01111101.00011110.00000101.11001000 .

In der Informatik hat sich die hexadezimale Schreibweise durchgesetzt, da sie am einfachsten zu handhaben ist. Die hexadezimale Schreibweise leitet sich folgendermaßen ab.
$2^8 = 2^4 \times 2^4$. Man erweitert das dezimale Zahlensystem bis zur Zahl 16 ($2^4$) durch die ersten Buchstaben des Alphabets.

10 = A
11 = B
12 = C
13 = D
14 = E
15 = F

Von Null bis F sind 16 Zahlen gleich $2^4$. In einer IP Adresse besteht eine Zahl aus acht binären Stellen xxxx xxxx. Diese lassen sich dann durch zwei vierstellige Zahlen darstellen.

00 = 0
0F = 15
10 = 16
1F = 31
20 = 32
..
FF = 255

Der Rechner kann die Eingabe der IP Adresse sowohl dezimal und binär als auch hexadezimal verstehen. Das oben genannte Beispiel lautet dann

125.30.5.200
01111101.00011110.00000101.11001000
7D.1E.05.C8

Diese Zahlenkombination sind als IP Adresse nicht so einfach strukturiert, dass der erste Rechner die Adresse 0.0.0.1 und der zweite Rechner die 0.0.0.2 erhält. Die IP Adressierung hat einen relativ komplizierten Aufbau.

# 4.3 Stationsadresse, Netzadresse, Subnet-Mask

Mit Hilfe der IP-Adressen kann ein Rechner den Standort eines anderen Rechners und den optimalen Weg (Routing) des Paketes dorthin ermitteln.

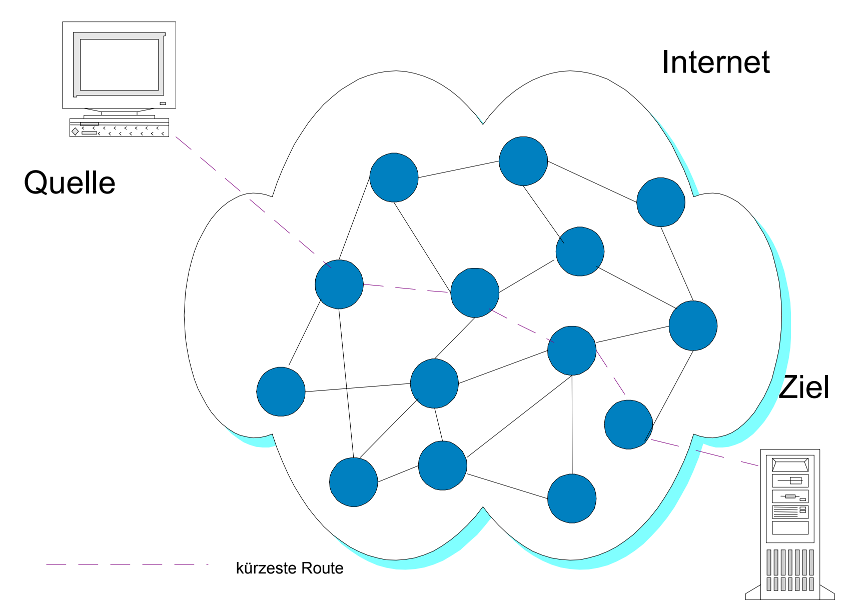



**Abbildung 4-1:** Ermittlung der kürzesten Route

Man kann das Adressenschema von Netzwerken verallgemeinern. Dies gilt für die meisten Netzwerkkommunikationsprotokolle.
Die Adresse eines Rechners im Netzwerk setzt sich aus drei Bestandteilen zusammen.
Der Netzadresse, der Knotenadresse und der Serviceadresse. Ein Vergleich mit dem globalen Telefonnetz dient zur Veranschaulichung
+49 30 39076500

| | | |
|---|---|---|
| +49 | Netzadresse | (Land) |
| 30 | Knotenadresse | (Stadt Berlin) |
| 39076500 | Serviceadresse | (Hallenbad, Rathaus, Einwohnermeldeamt, Polizei ...) |

Eine IP Adresse ist zweigeteilt. Der eine Teil stellt den Netzwerkanteil dar, der andere den Knotenanteil.

Beispiel
Die IP Adresse lautet 10.0.0.10
10.0 ist der Netzanteil
0.10 ist der Knotenanteil der IP Adresse

Es muss ganz deutlich werden, das in dem Netz 10.0 es einen Knoten gibt 0.10. Weiterhin ist es möglich, dass in einem Netz 11.0 ein Knoten 0.10 existieren kann. Dennoch können beide Knoten nicht miteinander in Verbindung treten, da sie sich in unterschiedlichen Netzen befinden. Vergleiche das Telefonbeispiel +49 30 ... und +33 (Frankreich) 30 (ein Dorf in Gallien). Zu den Serviceadressen kommen wir noch.

**Wer bestimmt nun, welcher Teil der IP Adresse Netz und welcher Knoten ist?**

Jede IP Adressierung besteht aus einer IP Adresse und der SUBNETMASK. Die SUBNETMASK bestimmt welcher Teil der IP Adresse Netz ist und welcher Knoten. Um die SUBNETMASK besser zu verstehen, benötigen wir die binäre Ansicht unserer dezimalen Zahlen.

Die SUBNETMASK hat den gleichen Aufbau wie die IP Adresse, also vier Zahlen (max. 255) durch Punkte getrennt ($2^8$ = 256 Zahlen). Die SUBNETMASK beginnt immer mit Einsen und endet immer mit Nullen. Beispiel für mögliche SUBNETMASKs.

11111111.00000000.00000000.00000000
11111111.11110000.00000000.00000000
11111111.11111111.00000000.00000000
11111111.11111111.11000000.00000000
....

Es kann keine Variation der Nullen und Einsen geben (beispielsweise 11001101.00111100.00000000.00001111). Die SUBNETMASK beginnt mit Einsen und geht dann willkürlich in die Nullen über.

**Wie ist der Zusammenhang zwischen der SUBNETMASK und der IP Adresse ?**

Die SUBNETMASK bestimmt, welche Stellen der IP Adresse Netzteil sein soll, und welcher Knotenteil.

Schreibt man IP Adresse und SUBNETMASK untereinander auf, wird schnell ersichtlich, welche Funktion die SUBNETMASK übernimmt.

| | |
|---|---|
| IP Adresse | 00001010.00000000.00000000.00001010 |
| SUBNETMASK | 11111111.11111111.11000000.00000000 |

Der unterlegte Bereich, der durch die Einsen markiert wird, gibt an, welche Stellen der IP Adresse Netz sein soll, der Rest ist dann der Knotenbereich. Kompliziert wird es nur, wenn man die IP Adresse in der dezimalen Ansicht betrachtet. Der Knoten 63.10 oder 62.10 haben den gleichen Netzanteil ( 00). Der Knoten 64.10 hat einen Netzanteil 01 und liegt in einem anderen Netz. 63.10 und 62.10 können miteinander kommunizieren, die 64.10 kann so einfach nicht erreicht werden. Um unterschiedliche Netze miteinander zu verbinden braucht man einen Router. Auf die Funktionsweise eines Routers wird hier nicht eingegangen, da dies den Rahmen der Unterlage sprengen würde.

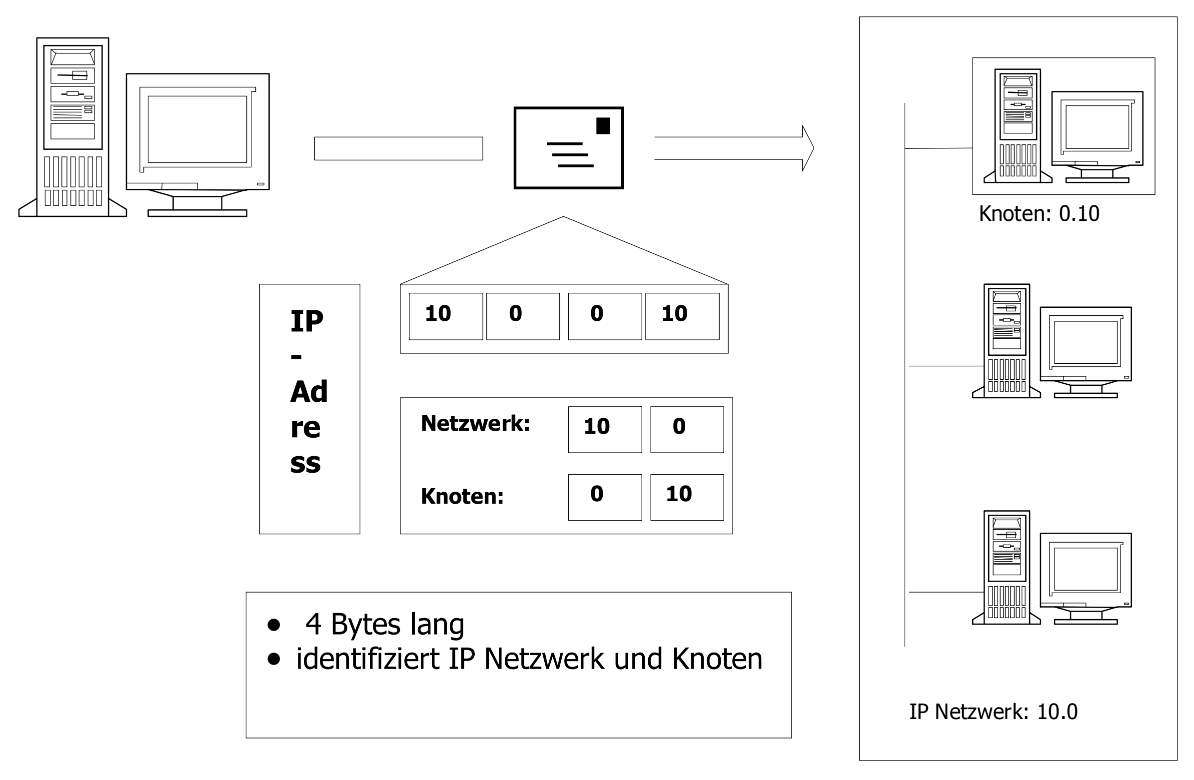



**Abbildung 4-2:** Aufbau einer IP-Adresse

Die Serviceadresse beschreibt, welcher Service durch die ankommenden IP Pakete angesprochen werden soll. Sollen die Daten auf die Festplatte abgespeichert werde, oder sollen sie ausgedruckt werden. Alle Dienste (auch FTP oder Telnet) verfügen über eigene Serviceadressen.

## 4.4 "Freie" (nicht routbare) IP-Adressen

IP-Adressen, die mit dem Internet verbunden sind, dürfen **grundsätzlich nicht frei gewählt werden**, da es hierdurch sehr schnell zu Adresskonflikten käme. Vielmehr werden IP-Adressen offiziell vergeben und zugeteit. Sie erhalten Ihre IP-Adresse(n) vom Internet-Provider, z.B. BelWÜ. Darüberhinaus gibt es für jede Netzklasse einen fest definierten Adressbereich, der für private Zwecke frei verwendet werden kann. Diese „freien" Adressen können jedoch nicht für eine direkte Internetverbindung genutzt werden, da IP-Datenpakete von Rechnern mit diesen Adressen von Routern nicht weitergeleitet werden. Wenn Sie diese Adressen in Ihrem LAN verwenden, müssen sie für einen Datenaustausch mit dem Internet in gültige, offizielle IP-Adressen umgesetzt werden. Dies kann online geschehen, indem der Kommunikations-Server in den Datenpaketen die IP-Adressen Ihrer Client-PC's durch seine eigene ersetzt. Dieses Verfahren heißt unter Linux **IP-Masquerading**, da die IP-Adressen der Clients wie unter einer Maske versteckt werden.

Folgende Adressen sind frei verwendbar und nicht routbar:



| | | |
|---|---|---|
| 10.0.0.0 | bis | 10.255.255.255 |
| 172.16.0.0 | bis | 172.31.255.255 |
| 192.168.0.0 | bis | 192.168.255.255 |

Darüberhinaus wird eine sog. *localhost*-Adresse definiert. Diese spricht immer den eigenen Rechner (localhost) an, unabhängig davon, welche IP-Adresse(n) ihm sonst noch zugeteilt wurde(n):

localhost : 127.0.0.1

## 4.5 Logische Rechnernamen

Da es den meisten Mensch schwer fällt, sich diese Unmengen von IP-Adressen zu merken, wurde im Internet von vornherein die Möglichkeit vorgesehen, Rechner zusätzlich zu den IP-Adressen auch noch mit frei wählbaren logischen Namen zu versehen.

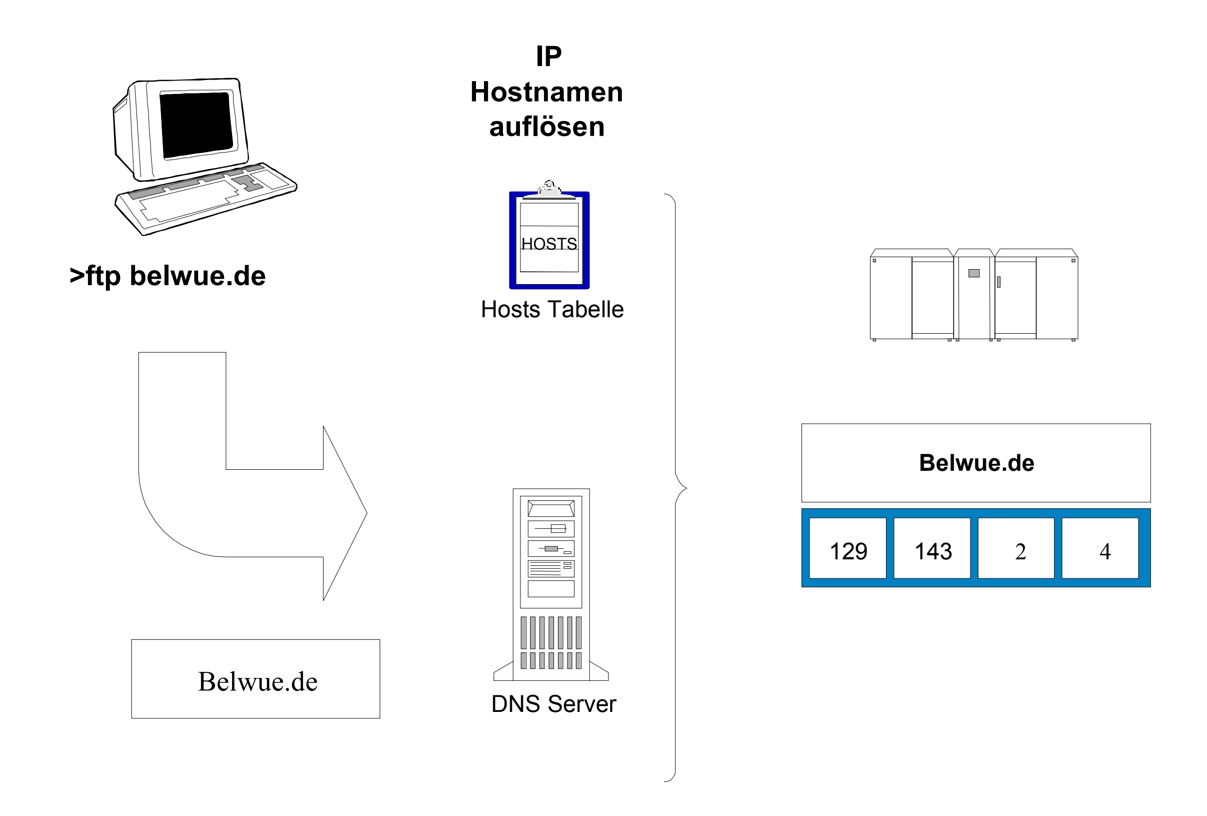



**Abbildung 4-3:** Zuordnung eines logischen Namens zu einer IP-Adresse

Diese Zuordnung kann zum einen über eine sog. Hosts-Tabelle erfolgen. In dieser Tabelle wird jedem Rechner eine eindeutige IP-Adresse und ein logischer Name zugewiesen. Wird das Netzwerk um einen Rechner erweitert, so muss die Hosts-Tabelle auf jedem Rechner




des Netzwerks angepasst werden. Bei großen Netzen ist diese Art der Netzwerkadministration nicht zu bewältigen. Diese Form der Vergabe von Rechnernamen in Tabellenform war im Internet sogar bis 1984 die einzig im Internet benutze Methode. Dabei wurden die Rechneradressen und Namen des gesamten Internet in den USA von einer einzigen Stelle, dem NIC (Network- Information-Centre), zentral verwaltet. Diese Tabelle wurde regelmäßig an die Server im Internet verteilt. Als das Internet allerdings immer stärker anwuchs, wurde der organisatorische Aufwand zu groß. Mit dem Domain-Name-Service (DNS) wurde ein neues Verfahren zur Adressierung von Rechnernamen eingeführt.

## 4.6 Domain-Name-Service (DNS)

Der DNS organisiert die Rechnernamen in einer Hierarchie von Domains, ähnlich dem UNIX-Dateisystem. Ausgangspunkt dabei ist eine gemeinsame Wurzel (engl. root). Darauf folgen die oberste Ebene (Top-Level-Domains) und weitere Ebenen (Subdomains). Unter einer Domain versteht man die Ansammlung von Rechnern, die nach organisatorischen oder geographischen Gesichtspunkten zusammengehören, wie bspw. alle Rechner eines Landes (Top-Level-Domain für Deutschland: de) oder alle Rechner einer Schule (schule).
Abbildung 4-4 zeigt ein Beispiel für eine solche Struktur (leu.bw.schule.de).

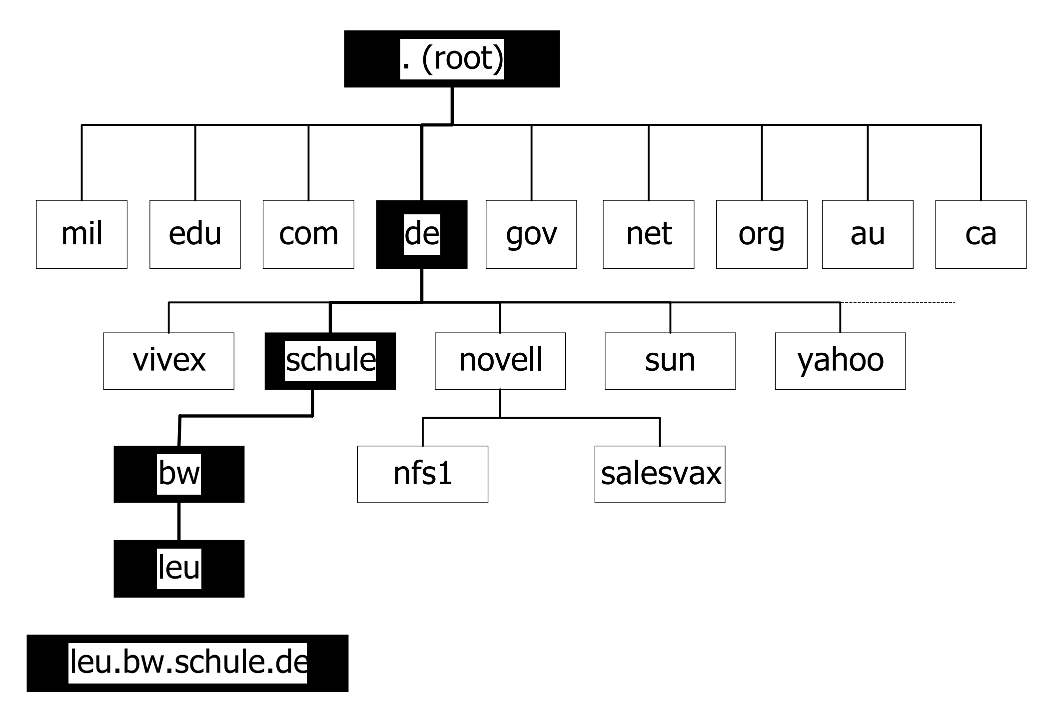



**Abbildung 4-4:** Beispiel einer Domain-Struktur

Bis zum Zeitpunkt der DNS-Konfiguration auf Ihrem Server können Sie z.B. in das Zielfeld eines Internet-Browsers auf den Client-PC's nur IP-Adressen angeben. Um anstelle der IP-Adressen als Ziel einen Namen, z.B. www.vivex.de eingeben zu können, muss eine Na-






mensauflösung erfolgen. Hierfür verwenden Sie den Domain Name Service, der dem sog. *Fully Qualified Domain Name* (FQDN) eines Rechners eine IP-Adresse zuordnet und umgekehrt. Der *Fully Qualified Domain Name* besteht aus dem Rechnernamen, gefolgt vom Pfad aller Internet-Domänennamen, die zu diesem Rechner führen.

DNS erlaubt die logische, hierarchische Strukturierung des Netzes, indem es Rechner im Netz zu Domänen zusammenfasst und diese Domänen zu einem Domänen-Verzeichnis-Baum (DVB), ähnlich einem Dateisystem, verschachtelt. An der Spitze der Hierarchie stehen Domänen wie "com" oder "de" für "Commercial (USA)" bzw. "Deutschland", während die niedrigste Ebene diejenige ist, in der sich der betreffende Rechner befindet.

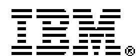
Wenn Sie DNS verwenden, werden alle beteiligten Rechner im eigenen Netz, d. h. in der eigenen Domäne, untereinander bekannt gemacht. Zur Auflösung von Rechnernamen, die nicht zur eigenen Domäne gehören, wird die Anfrage an die nächste Domäne weitergereicht.

Der Domain Name Service ist eine Client-Server-Anwendung. Die Clients werden als sog. *Resolver*[7] bezeichnet, die Server als *Name-Server*. Die Name-Server beinhalten die Listen, in denen IP-Adressen auf Rechnernamen abgebildet werden und umgekehrt. Sie werden Ihren Linux-Server als Cache-Name-Server konfigurieren, d.h. Ihr Server befragt zur Namensauflösung den nächsten Name-Server, welcher durch Ihren Internet-Provider gestellt wird und behält die gewonnenen Informationen im lokalen Cache (=Zwischenspeicher). Sie verwenden keinen vollwertigen Name-Server, da ein Name-Server regelmäßig (ca. alle 15 Minuten) seine Adresslisten mit anderen Name-Servern abgleicht. Sie müßten dementsprechend regelmäßig eine Verbindung zum nächsten Name-Server aufbauen, selbst wenn sonst keine Notwendigkeit für eine Verbindung zum Provider besteht.

Das DNS-Caching auf Ihrem Linux-Server ist also das Zwischenspeichern von DNS-Informationen, so dass bei wiederholten Zugriffen Ihrer Clients auf dasselbe Ziel im Internet zur Namensauflösung die zwischengespeicherten Informationen verwendet werden. Eine Verbindung zum Provider ist damit nicht notwendig.

Wenn Clients vom Internet die Namen der Rechner *Ihrer* Domäne auflösen wollen, müssen diese in die entsprechenden Tabellen des Name-Servers für Ihre Domäne eingetragen werden. Diese Aufgabe übernimmt Ihr Internet-Provider, also z.B. BelWü.

[7] resolve = auflösen



# 5 Installation und Grundkonfiguration eines Linux-Servers

Aufgrund der Kürze dieses Kurses werden Sie in diesem Kurs auf den Übungsrechnern ein bereits vorinstalliertes Linux vorfinden. Die Linux-Installation wurde ausführlich im Grundkurs besprochen. Wenn Sie am Grundkurs nicht teilgenommen haben sollten, finden Sie im folgenden Kapitel und in der zugehörigen Übung die vollständige Beschreibung der für diesen Kurs verwendeten Installation.

## 5.1 Hardware-Voraussetzungen

Im Gegensatz zu anderen PC-Betriebssystemen ist Linux in Bezug auf die Hardwareanforderungen sehr genügsam. Allerdings sind die Anforderungen an die Hardwareausstattung des Linux-Rechners abhängig vom geplanten Einsatzgebiet. So sind die Hardwarevoraussetzungen für einen Netzwerk- und Daten-Server ganz andere als für eine Linux-Workstation mit X-Window-Applikationen.

Obwohl Linux ursprünglich auf einen 386er INTEL-Prozessor programmiert wurde, unterstützt es mittlerweile eine große Bandbreite unterschiedlicher Prozessoren verschiedener Hersteller. Darüber hinaus werden alle gängigen Bussysteme (z.B. ISA-Bus, EISA, VLB, PCI) außer der Microchannel-Architektur (MCA) von IBM unterstützt. Auch auf Festplattenseite ist der Hardwareanspruch nicht besonders hoch. Alte Festplatten, wie MFM oder RLL werden genauso unterstützt, wie die heute üblichen IDE-, EIDE- und SCSI-Festplatten, wobei meistens SCSI-Festplatten bevorzugt werden. Ihr Linux-System sollte, nicht nur zur Installation, mit einem CD-ROM-Laufwerk ausgestattet sein. Einzig CD-ROM-Laufwerke, die über eine parallele Schnittstelle angeschlossen sind, bereiten Schwierigkeiten. Ansonsten werden alle Laufwerke mit dem ATAPI-Standard, alle SCSI-Laufwerke und die meisten IDE-CD-ROM-Laufwerke unterstützt. Ähnlich wie bei den Bussystemen kann Linux mit den meisten Grafikcontrollern zusammenarbeiten. Die Grafikkarten-Relikte wie MDA, Herkules, CGA und EGA werden genauso unterstützt, wie die heute üblichen VGA- und Super-VGA-Grafikkarten. Auch bei den Netzwerkkarten können praktisch alle gängigen Standards, wie Ethernet oder Token-Ring benutzt werden.

Im Verzeichnis `/usr/doc/HOWTO`, das ganz nach Standart installiert wird, können Sie wertvolle Hinweise und Listen von Komponenten finden, die von Linux unterstützt werden.

Die folgende Liste zeigt die wichtigsten Leistungsmerkmale eines Linux-Servers.

Pentium 166
64 MB RAM
4 GB SCSI-Festplatte
VGA-Standard Grafikkarte
15"-Farbmonitor
10/100 MBit-Netzwerkkarte
CD-ROM SCSI
3 ½" Diskettenlaufwerk
Tastatur
DAT-Laufwerk, SCSI

Leistungsmerkmale eines Linux-Servers

## 5.2 Installation des Linux-Grundsystems

Um den Rahmen dieser Unterlage nicht zu sprengen, sei für die Installation des Linux-Grundsystems an dieser Stelle auf die Übung 5-1 im Übungsteil verwiesen.

Unter Linux wird Software in sog. *Pakete* verpackt, die Installation setzt demnach das Einspielen der gewünschten Pakete voraus. In diesem Kurs wird die S.u.S.E.-Version 5.2 benutzt, welche 22 Paketserien enthält, in denen ca. 620 Einzelpakete nach Anwendungsgebieten thematisch zusammengefasst sind.

Es ist für die verwendete Installation nicht nötig, einzelne Pakete oder Serien manuell auszuwählen. Vielmehr können Sie während der Installation eine sog. *Konfiguration* laden, die den Anwendungszweck Ihrer Installation beschreibt. Wir verwenden die beiden Konfigurationen:

- default (ist bei jeder Installation voreingestellt)
- InterSrv * Internet access server system

Sie benötigen für diese Installation ca. 300 MB freien Festplattenplatz. Hinzu kommen ca. 1 GB Plattenplatz für den Proxy- und Web-Server.

---

 **Übung 5-1:** Installation von Linux

---

## 5.3 Einspielen/Entfernen von Paketen

Wenn Sie weitere Pakte einspielen oder vorhandene entfernen wollen, melden Sie sich als Systemverwalter *root* an und starten das S.u.S.E.-Setup-Tool `YAST` mit der Eingabe von `yast` in der Commandozeile. Im Hauptmenü können Sie *über* `<Installation festlegen / starten>` den Umfang der zu installierenden Pakete festlegen und die Installation starten.

```
YaST - Yet another Setup Tool
YaST Version 0.89.1 -- (c) 1994-98 S.u.S.E. GmbH

Sprache:       Deutsch
Quellmedium:   CD-ROM ATAPI EIDE /dev/hdb
Root-Device:   /dev/hda2

Allgemeine Hilfe zu Installation und YaST-Tastaturbelegung
Einstellungen zur Installation                            ->
Installation festlegen/starten
System updaten
Administration des Systems                                ->
README-Datei zum Installationsmedium anzeigen
Copyright
YaST beenden
```

**Abbildung 5-1:** Setup-Tool `YAST`

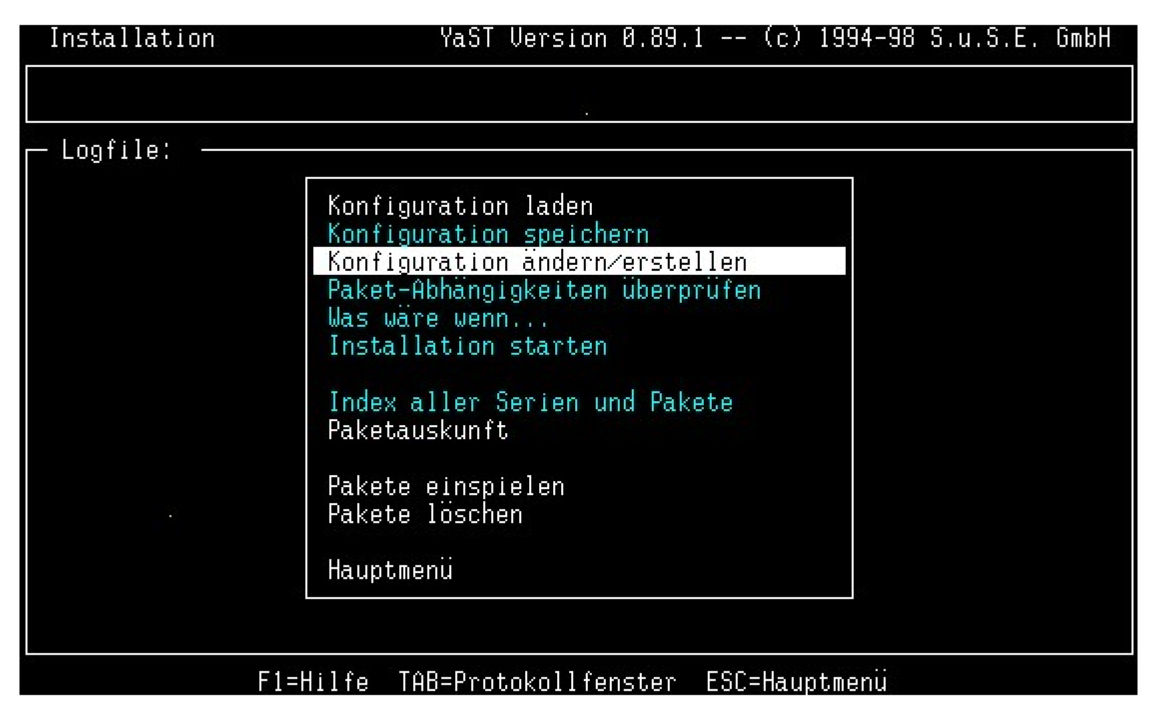



**Abbildung 5-2:** Ändern der Konfiguration

Über den Menüpunkt `<Konfiguration ändern/ erstellen>` können Sie dann ihr System auf Ihre Bedürfnisse anpassen und somit Pakete deinstallieren, aktualisieren oder neu hinzufügen. Sie gelangen in die Serienauswahl, in der Sie über die Cursortasten eine Paketserie zur weiteren Bearbeitung anwählen können.

Mit Auswahl der Paketserie `**n**` (Netzwerk-Support) gelangen Sie beispielsweise in das Auswahlmenü der Einzelpakete, aus denen sich die Paketserie `**n**` zusammensetzt.

Über die Cursortasten können Sie die einzelnen Pakete anwählen. Im unteren Fenster erscheint dann jeweils eine kurze Beschreibung mit Versionsnummer und Paketgröße des Paketes. Vor den Paketen wird in eckigen Klammern der jeweilige Status angezeigt:

[ ] ⇒ Paket ist noch nicht installiert

[ X ] ⇒ Paket ist zu installieren

[ i ] ⇒ Paket ist bereits installiert

[ D ] ⇒ Paket ist zu löschen

[ R ] ⇒ Paket ist zu aktualisieren.

Nach Auswahl der benötigten Pakete mit Hilfe der Leertaste wird die Installation über den Menüpunkt <Installation starten> durchgeführt.

## 5.4 Konfiguration des Netzwerks

### 5.4.1 Voraussetzungen

Linux unterstützt verschiedene Netzwerkkarten (Ethernet, Arcnet, TokenRing) und kennt fast alle gängigen Netzwerkprotokolle (TCP/IP, IPX; Apple Talk). Wir gehen in diesem Fall von einem Linux-Rechner mit einer Ethernetkarte in ein TCP/IP-Netzwerk aus. Aktuellste Informationen bezüglich anderer Netzwerke finden Sie u.a. im Verzeichnis `Documentation` bei den Kernelquellen (/usr/src/linux); darüber hinaus liefert die Hilfefunktion beim Konfigurieren des Kernels äußerst wertvolle weitere Informationen.

Die folgenden Voraussetzungen müssen erfüllt sein:

- Der Rechner muss über eine unterstützte Karte verfügen.
  Ob die Karte korrekt erkannt wurde, können Sie unter anderem daran sehen, dass die Ausgabe des Kommandos

  ```
  cat /proc/net/dev
  ```

  eine Zeile enthält, die mit `eth0:` beginnt.

- Der Kernel muss für das zu verwendende Netz korrekt konfiguriert sein.

Sind diese Voraussetzungen erfüllt, so sollten vor der Netzwerkkonfiguration noch folgende Punkte geklärt werden:

| | |
|---|---|
| `Rechnername` | Name, den der Rechner im Netzwerk haben soll. Der Name sollte nicht länger als acht Zeichen sein und darf im lokalen Netzwerk noch nicht vergeben worden sein. |
| `Domainname` | Der Name der Domain, der der Rechner angehören wird. |
| `IP-Adresse` | Die IP-Adresse des Rechners im Netzwerk. |
| `Gatewayadresse` | Wenn sich im Netzwerk ein als Gateway fungierender Rechner befindet, d.h. ein Rechner, der in mehr als einem Netz hängt und der das Weiterleiten von Netzwerkpakete in das fremde Netz übernimmt, so kann dessen Adresse bei der Netzwerkkonfiguration angegeben werden. |

| | |
|---|---|
| `Netzwerkmaske` | Mit Hilfe der Netzwerkmaske (netmask) wird entschieden, in welchem Netzwerk eine vergebene Adresse zu finden ist. Die Adresse wird mit der Netzwerkmaske durch ein logische *UND* verknüpft, wodurch der Host-Anteil der Adresse ausgeblendet wird, so dass nur noch die Adresse des Netzwerkes übrig bleibt. |
| `Adresse des Name-Servers` | Name-Server stellen den Dienst (DNS, DomainName-Service) zur Verfügung, mit dem sich Rechnernamen in IP-Adressen wandeln lassen. Ist ein Name-Server über das Netz zu erreichen und soll dieser verwendet werden, so kann dessen IP-Adresse bei der Netzwerkkonfiguration angegeben werden. |

### 5.4.2 Einbau einer zweiten Netzwerkkarte

Aufgrund der Datensicherheit sollte das schulinterne Computernetz physikalisch vom Internet getrennt werden. Dafür ist es erforderlich, dass in den Server zwei Netzwerkkarten eingebaut sind, so dass eine Karte ausschließlich mit dem LAN verbunden ist und die zweite mit dem Internet (bzw. Router zum Internet).
Zum Einbau der Netzwerkkarte müssen Sie den Server mit dem Befehl <*shutdown -h now*> herunterfahren. Wenn die Vollzugsmeldung erscheint, schalten Sie den Rechner aus. Anschließend sollten Sie das Netzkabel (Strom) des Rechners ziehen.

---

***Achtung**: Das Ansprechen zweier Netzwerkkarten ist unter Linux nicht einfach. Verwenden Sie möglichst keine identischen ISA-Karten, sondern Karten, die verschiedene Treibermodule benötigen (z.B. NE2000 und 3COM). Ebenfalls erfolgversprechend sind PCI-Netzwerkkarten. Bemühen Sie jedoch vor einer Neuanschaffung die S.u.S.E.-Support-Datenbank, ob die betreffenden Karten von Linux unterstützt werden! Wenn Sie die Konfiguration "Internet Access Server" installiert haben, wird ein Teil dieser Support-Datenbank als HTML-Dokumentensammlung von Ihrem Apache-Web-Server zur Verfügung gestellt.*

---

Vor dem Einbau sollten Sie die Input/Output-Adresse (I/O) und den Interrupt (IRQ) der Karte ermitteln (Anleitung lesen) und notieren.

---

***Achtung**: Ihre beiden Netzwerkkarten müssen verschiedene Ressourcen belegen, d.h. IRQ und I/O müssen sich voneinander unterscheiden und dürfen in keinem Adreß-Konflikt mit anderen Geräten im System stehen! Sie müssen ggf. die zweite Karte mit der vom Hersteller mitgelieferten Software umkonfigurieren*

---

Nach dem Verschließen des Rechners fahren Sie Linux wieder hoch und starten `Yast`. Unter dem Menüpunkt `<Administration des Systems>`, dem Untermenü `<Hardware in das System integrieren>` und `<Netzwerkkarte konfigurieren>` können Sie die zweite Netzwerkkarte in das System einbinden. Detaillierte Informationen hierzu finden Sie in der folgenden Übung.

Nach dem Einbau der zweiten Netzwerkkarte wird Ihr Netz in etwa wie folgt konfiguriert sein:

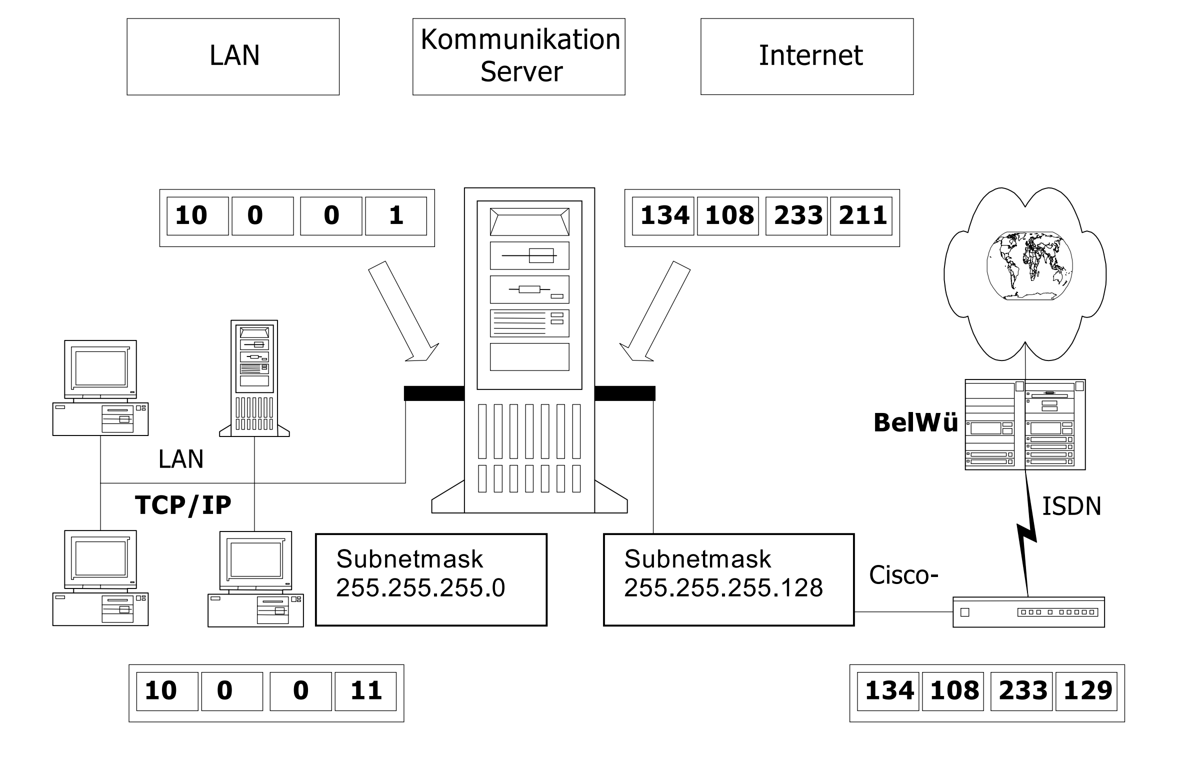



**Abbildung 5-3:** Netzkonfiguration bei Verwendung von zwei Netzwerkkarten und nicht routbaren IP-Adressen im lokalen Netz



## **Übung 5-2:** Einbau einer zweiten Netzwerkkarte

### 5.4.3 IP-Masquerading

Prinzipiell wäre Ihr Linux-Server jetzt in der Lage, Kunden (clients) aus dem lokalen Netz mit dem Internet zu verbinden. Dies ist möglich, da er als Router arbeitet, also IP-Datenpakete aus dem lokalen Netz ins Internet weiterleitet und umgekehrt. Wenn Sie nun aber im lokalen Netz freie (nicht routbare) Adressen verwenden, so kommen diese Datenpakete nicht über den ersten "offiziellen" Router hinaus – das wäre der Cisco-Router in Ihrem Haus.

Um dieses Problem zu lösen, kann Ihr Linux-Server IP-Adressen umsetzen. Er ersetzt in Datenpaketen, die vom LAN ins Internet gelangen sollen, die IP-Adresse der absendenden Arbeitsstation durch seine eigene. Der Linux-Server muss sich dabei merken, welche Arbeitsstation eine Anfrage ins Internet gesendet hat. Wenn die angeforderten Daten zurückkommen, muss nämlich er als vermeintlicher Absender wieder seine IP-Adresse durch diejenige der anfragenden Arbeitsstation ersetzen.

Das funktioniert natürlich auch dann, wenn Sie im LAN "echte", vom BelWü zugeteilte IP-Adressen verwenden. In jedem Fall kommen aus der Sicht des Internets Anfragen immer nur von Ihrem Linux-Rechner, d.h. von dessen IP-Adresse. Alle anderen Rechner in Ihrem LAN sind somit für das Internet unsichtbar, sie tragen eine "Maske".

Beim Masquerading werden also lokale IP-Adressen versteckt., d.h. außerhalb des lokalen Netzes wird ausschließlich die IP-Adresse des Masquerading-Rechners angezeigt.

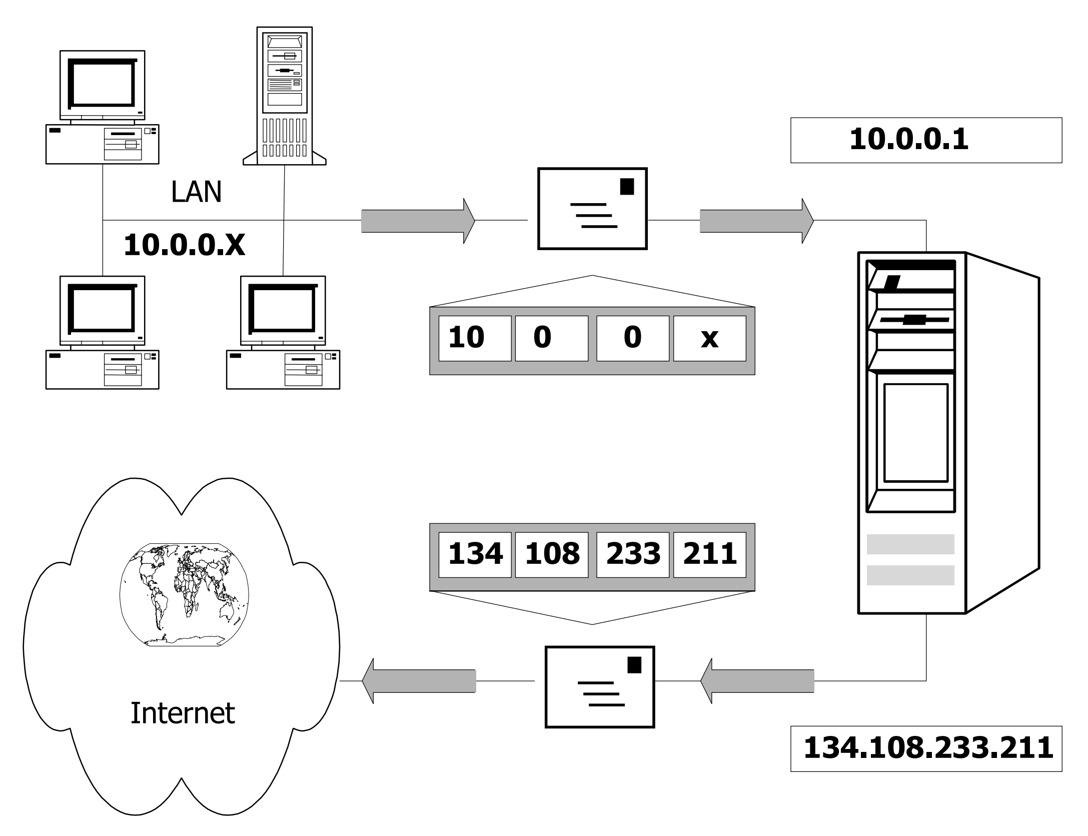



**Abbildung 5-4:** Prinzip des IP-Masquerading

Die Maske kann einerseits dazu benutzt werden, die Architektur des lokalen Netzes zu verhbergen. Andererseits, um einem Netz, das über keine eigene IP-Adresse verfügt, den Zugang zum Internet zu ermöglichen. Bei vielen Internet-Providern wird dieses Verfahren praktiziert, d.h. die Kunden wählen sich beim Provider ein, bekommen eine IP-Adresse zugewiesen und arbeiten solange unter dieser Adresse. Die eigenen, internen Adressen treten nicht in Erscheinung.

Das Masquerading wird über das Setzen von Variablen in der systemweiten Konfigurationsdatei **/etc/rc.config** gesteuert. Diese Variablen können Sie am Präfix `MSQ_` erkennen.

| | |
|---|---|
| <MSQ_START> | Dieser Wert muss auf `yes` geändert werden, damit das Masquerading gestartet wird. |
| <MSQ_DEV> | Device, auf dem das Masquerading laufen soll. |
| <MSQ_NETWORKS> | Liste der lokalen Netze, die "versteckt" werden sollen. |
| <MSQ_MODULES> | Module, die zum Masquerading geladen werden sollen.<br>Es gibt die drei Module<br>Ip_masq_FTP für FTP<br>Ip_masq_irc für IRC<br>Ip_masq_raudio für Real-Audio |

Variablen in der Datei `/etc/rc.config` für das Masquerading

Wenn Sie das Masquerading aktiviert haben, wird es bei jedem Systemstart automatisch durch ein entsprechendes Skript gestartet. Dieses können Sie auch manuell aufrufen. Das *masquerading-skript* unter S.u.S.E.-Linux kennt zwei Parameter zum Start des Firewalls:

| | |
|---|---|
| `Start` | Masquerading wird gestartet |
| `Stop` | Masquerading wird abgeschaltet |

Beispiel zur Aktivierung des Masqueradings:

**/sbin/init.d/masquerade start [↵]**

Ihre Datei `/etc/rc.config` wird also bei aktiviertem Masquerading folgende Einträge aufweisen:

```
#
# Masquerading settings - See /usr/doc/packages/firewall
#                          for a detailed description
#
MSQ_START="yes"
MSQ_NETWORKS="10.0.0.0/255.255.255.0"
MSQ_DEV="eth0"
MSQ_MODULES="ip_masq_cuseeme  ip_masq_FTP  ip_masq_irc  ip_masq_quake
ip_masq_raudio ip_masq_vdolive"
```

---

***Achtung:*** *Im Parameter* `MSQ_NETWORKS` *geben Sie* ***Netzwerk****nummer und –maske Ihres* ***lokalen*** *Netzes an; die IP-Adressen dieses Netzes werden versteckt. Im Parameter* `MSQ_DEV` *hingegen geben Sie die Netzwerkkarte an, die mit dem* ***Internet*** *(bzw. Cisco-Router) verbunden ist; auf dieser Karte wird die Adressumsetzung durchgeführt.*

---



**Übung 5-3:** Aktivierung des IP-Masqueradings

---

# 6 Konfiguration der Client-PC's (TCP/IP und DNS)

Ihr Linux-Server ist nun in der Lage, Ihr lokales Netz mit dem Internet zu verbinden. Damit die Client-Rechner im LAN auf den Linux-Server und das Internet zugreifen können, müssen sie das TCP/IP-Protokoll verwenden. Die entsprechende Konfiguartion wird im folgenden Kapitel besprochen.

## 6.1 Windows 95 und Windows NT

In dieser Schulung werden „Windows 95-PCs" eingesetzt, da sie an den meisten Schulen benutzt werden. Im Lieferumfang von Windows 95 ist bereits das TCP/IP Protokoll enthalten. Man muss es nur noch konfigurieren. Das zugehörige Menü können Sie z.B. aufrufen, indem Sie mit der rechten Maustaste auf das Symbol *Netzwerkumgebung* auf Ihrem Desktop klicken und aus dem Konextmenü *Eigenschaften* auswählen.

Die Konfiguration erfolgt in drei verschiedenen Registerkarten:

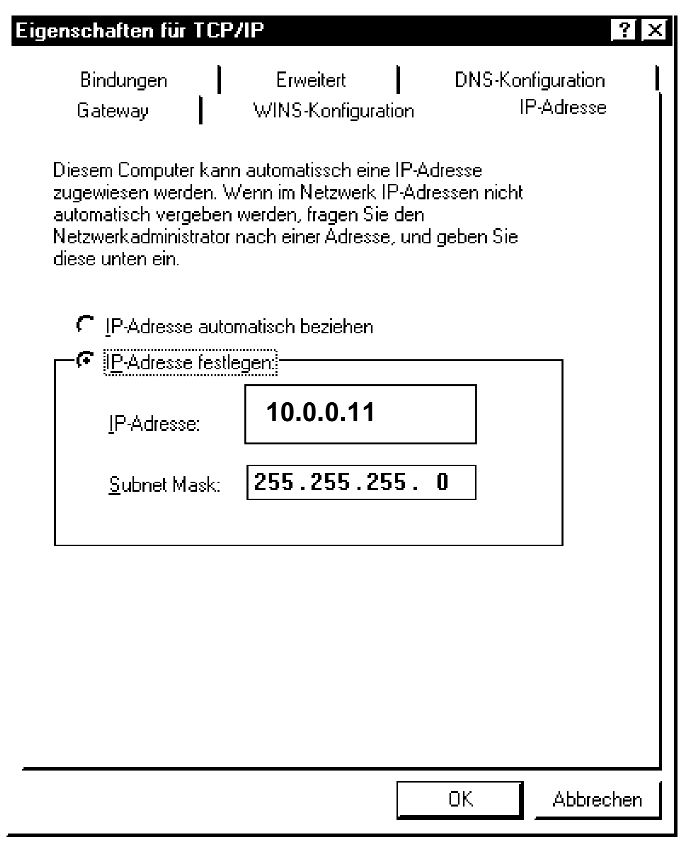



**Abbildung 6-1:**TCP/IP Konfiguration

1) Im Registerblatt **IP-Adresse** werden die IPAdresse und die Subnet-Mask eingetragen.

2) Im Registerblatt **DNS-Konfiguration** werden die zur Nutzung von DNS notwendigen Einträge vorgenommen.

3) Die Einstellungen zum Default-Gateway werden in der Registerkarte **Gateway** eingetragen. Hier wird die IP-Adresse des Default-Gateways eingetragen. Dieses ist die IP-Adresse der dem lokalen Netz zugewandten Netzwerkkarte (eth1) Ihres Linux-Servers.

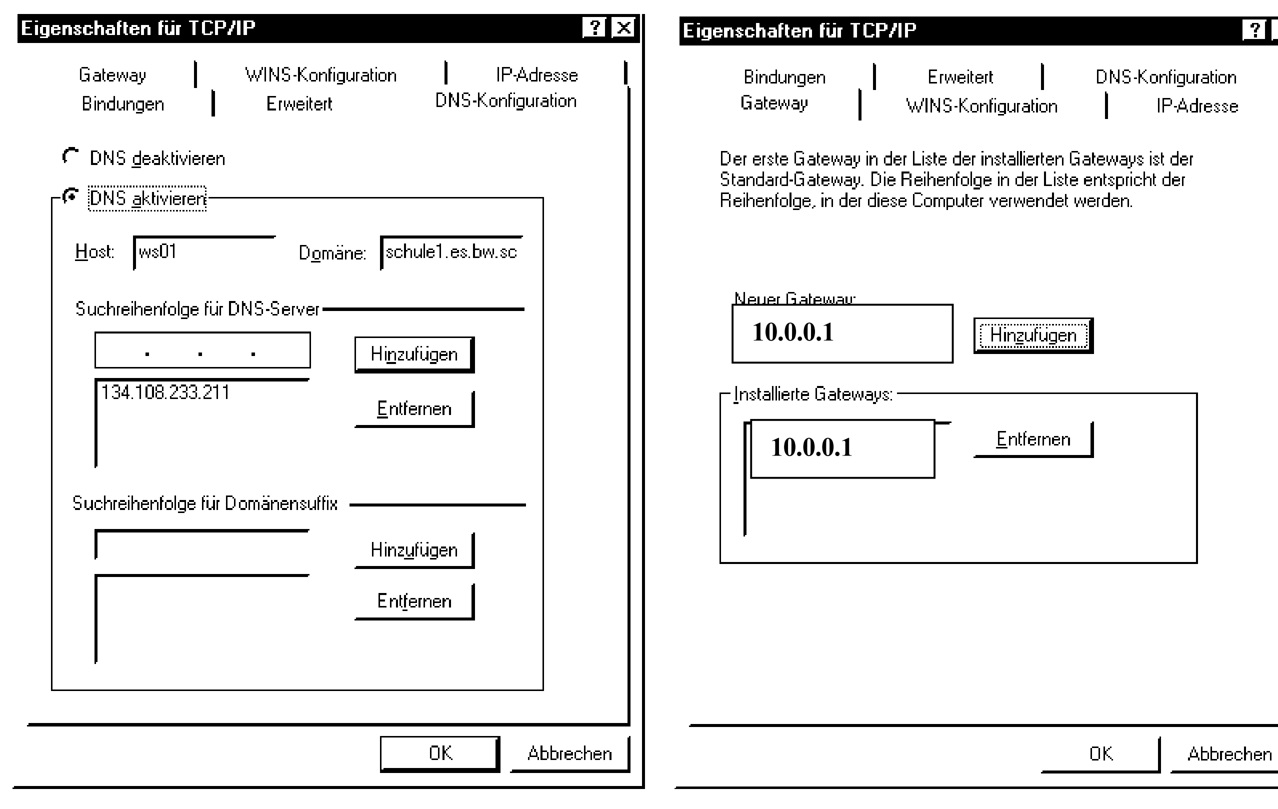



**Abbildung 6-2:** DNS-und Gateway-Konfiguration unter Windows 95



## **Übung 6-1:** TCP/IP-Konfiguration der Client-PC's

## 6.2 Netscape Communicator Installationsschritte

Um Ihre Netzwerk-Konfiguration zu testen, werden Sie nun als Internet-Browser den Netscape Communicator[8] installieren. Er dient zur Anforderung von Webseiten aus dem Internet. Sie werden ihn verwenden, um zunächst auf den Apache-Web-Server[9] zuzugreifen, der auf Ihrem Linux-Server installiert ist. Anschließend werden Sie Webseiten aus dem Internet anfordern und damit die vollständige Konfiguration Ihres Servers testen, da hierfür Routing, IP-Masquerading und später auch Namensauflösung über den DNS-Server verwendet werden müssen.

In Tabelle 6-1 sind die wesentlichen Schritte zur Installation und Konfiguration des Netscape Communicators dargestellt. Die Tabelle beinhaltet außerdem die Ergebnisse jeden Schrittes sowie das zur Durchführung benötigte Utility bzw. Kommando. Die detaillierte Installationsanweisung finde Sie in der **Übung 6-2**.

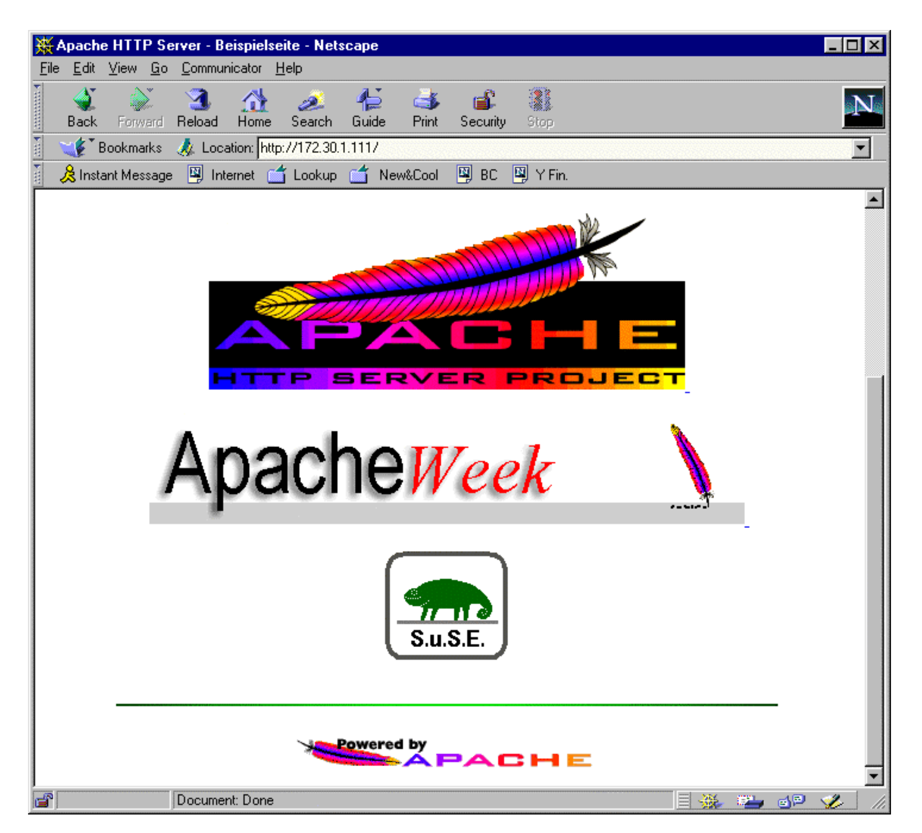



**Abbildung 6-3:** Mit dem Netscape Navigator können Sie auf Ihren Web-Server zugreifen

[8] kostenlos im Internet erhältlich unter http://home.netscape.com/download/
[9] Der Web-Server "Apache" läuft bereits nach der Standardinstallation von Linux.



| Installationsschritt | Ergebnis | Utility/Kommando |
|---|---|---|
| 1) Führen Sie die Netscape-Datei CC32E404.EXE für Windows 95 aus. | Kopiert die benötigten Dateien und konfiguriert die Benutzerumgebung, um den Netscape Browser verwenden zu können. | CC32E404.EXE |
| 2) Starten Sie den Browser. | Aufforderung zum Anlegen eines Benutzerprofils. | NETSCAPE.EXE |
| 3) Legen Sie das Standard-Benutzerprofil "default" an. | Alle Benutzereinstellungen für den Navigator werden im Profil "default" gespeichert. | NETSCAPE.EXE |
| 4) Tragen Sie ggf. einen Proxyserver ein und setzen Sie den lokalen Netscape-Cache auf Null. | Beschleunigt den Zugriff auf Informationen im Internet. | NETSCAPE.EXE (Edit→Prefrences...) |
| 5) Begeben Sie sich auf die Homepage Ihres Web-Servers. | Gibt Ihnen die Möglichkeit, Informationen des "Apache" Web-Servers zu sehen. | NETSCAPE.EXE |

**Tabelle 6-1:** Netscape Browser Installationsschritte

---



**Übung 6-2:** Installation des Netscape Communicators

---

# 7 Domain Name Service (DNS)

Sie können in das Adressfeld Ihres Internet-Browsers nur eine IP-Adressen angeben, bis Sie die DNS auf Ihrem Server konfiguriert haben. Um anstelle der IP-Adressen als Ziel einen Namen, z.B. www.vivex.de, eingeben zu können, muss eine Namensauflösung erfolgen. Hierfür verwenden Sie den Domain-Name-Service, der dem sog. *Fully Qualified Domain Name* (FQDN) eines Rechners eine IP-Adresse zugeordnet und umgekehrt. Der *Fully Qualified Domain Name* besteht aus dem Rechnernamen, gefolgt vom Pfad aller Internet-Domänennamen, die zu diesem Rechner führen. Weitere Informationen zum Thema Domain-Name-Service Grundlagen finden Sie im Kapitel 4.6.

## 7.1 Konfigurationsdateien für den DNS

Nachfolgend werden Ihnen übersichtsweise alle Konfigurationsdateien vorgestellt, die beim Domain Name Service verwendet werden bzw. verwendet werden können. Weitere Informationen finden Sie im Kapitel 4.

a) **`/etc/rc.config`**

Die Datei `/etc/rc.config` ist eine allgemeine S.u.S.E.-Linux-Konfigurationsdatei und enthält einige grundlegende Parameter, die für den DNS-Start notwendig sind.

b) **`/etc/host.conf`**

Die Datei `/etc/host.conf bestimmt`, über welche Methode Internet-Namen 'aufgelöst' wird, also in IP-Adressen umgewandelt werden. Dies kann über die Tabelle `/etc/hosts` erfolgen und/oder über den Namens-Dienst *Berkeley Internet Name Domain* `bind`, der als Namens-'Dämon' `named` implementiert und bei der verwendeten Konfiguration (Internet access server) bereits installiert ist.

c) **`/etc/hosts`**

Sie ist eine einfache Tabelle, in der Rechnernamen und zugeordnete IP-Adressen aufgelistet werden. */ etc / hosts /* ist immer vorhanden und enthält mindestens einen Eintrag für den eigenen Rechner. Es kann um weitere Einträge erweitert werden, wenn die Verwendung der `hosts`-Tabelle in der Konfigurationsdatei `/etc/host.conf` angezeigt ist.

d) **/etc/named.boot**

Dies ist eine sog. 'Ladedatei' für den Namens-Dämonen `named`. Sie wird beim Starten des `named` gelesen und enthält dessen Konfigurationsparameter.
Wenn Sie einen 'vollwertigen' Name-Server implementieren, dann werden vom `named` folgende weitere Dateien benötigt:

| | | |
|---|---|---|
| - eine 'Rechnerdatei' | z.B.: | `/var/named/named.hosts` |
| - eine 'umgekehrte Rechnerdatei' | z.B.: | `/var/named/named.rev` |
| - eine 'Loopback-Rechnerdatei' | z.B.: | `/var/named/named.local` |
| - eine 'Datei der Internet-Root-Server' | z.B.: | `/var/named/root.cache` |

e) Optional: Wenn Sie anstelle eines Name-**Servers** einen sog. Name-**Resolver** implementieren: `/etc/resolv.conf`

In der `/etc/resolv.conf` werden der Name-Server sowie der Name Ihrer Domäne eingetragen.

## 7.2 Einrichtung eines DNS-Cache-Servers

Für Ihre Schule ist es völlig ausreichend, wenn Sie lediglich einen sog. *DNS-Cache-Server* einrichten. Dieser legt DNS-Informationen in seinem Zwischenspeicher (Cache) ab. Die benötigte Information muss zunächst von einem anderen DNS-Server besorgt werden, welcher von Ihrem Provider (BelWü) betrieben wird. Erneute Anfragen auf dasselbe Ziel können dann aus dem Cache bedient werden, so dass hierfür keine Verbindung zum Provider aufgebaut werden muss.

### 1) Editieren der Datei `/etc/rc.config`

Tragen Sie in der Datei `/etc/rc.config` ein, so dass beim nächsten Systemstart der Namensdämon `named` gestartet wird:

```
#
# start the named (package bind)? You have to configure the named
# first, before you can start it (man named).
#
START_NAMED=yes
```

Tragen Sie außerdem Ihren Domänennamen (z.B. schule1.alf.es.bw.schule.de) in den Parameter `SEARCHLIST` ein. Im Parameter `NAME-SERVER vermerken Sie`, von welchem Name-Server Sie Informationen für die Namensauflösung bei lokalen Anfragen, z.B. von

*nslookup,* beziehen[10]. Hier können Sie Ihren Rechner eintragen (localhost, IP 127.0.0.1), der ja als DNS-Cache-Server arbeiten wird. Der zugehörige Abschnitt sieht dann in etwa wie folgt aus:

```
#
# domain searchlist that should be used in /etc/resolv.conf
# (e.g. "suse.de linux.de uni-stuttgart.de")
# Attention! this has to be filled out, if you want to access a name
# server
#
SEARCHLIST="schule1.alf.es.bw.schule.de"
#
# space separated list of Name-Servers that should be used for
# /etc/resolv.conf
# give a maximum of 3 IP numbers
# (e.g. "192.168.116.11 192.168.7.7")
#
NAME-SERVER="127.0.0.1"
#
```

## 2) Editieren der Datei `/etc/named.boot`

In der Ladedatei `/etc/named.boot` für den Namens-Dämon `named` werden folgende vier Zeilen benötigt:

```
directory /var/named
cache . root.cache
forwarders 129.143.2.4
slave
```

Die erste Zeile gibt an, in welchem Verzeichnis sich die Konfigurationsdateien befinden,die zweite Zeile aktiviert das Caching und verweist in der Datei `root.cache` auf die DNS-Root-Server im Internet (`root.cache` wird mit Linux mitgeliefert).
Die dritte Zeile gibt an, wer für Namensauflösungen befragt werden soll, wenn sich die Information *nicht* im Cache befindet (der Name-Server von BelWü mit der IP-Adresse 129.143.2.4).
Die letzte Zeile verhindert, dass zur Namensauflösung DNS-Root-Server befragt werden.

[10] Beide Parameter werden lediglich für die Resolver-Konfiguration verwendet, d.h. beim Aufruf von *nslookup* (s.h.) auf dem lokalen Linux-Rechner. Alle Anfragen von Client-Rechnern nimmt der Namens-Dämon *named* entgegen, den Sie über die Datei `/etc/named.boot` konfigurieren.






## 3) Aktualisieren der Konfiguration

Nach jeder Änderung in der Datei `/etc/rc.config` sollten Sie **`/sbin/SuSEconfig`** aufrufen, damit eventuell notwendige weitere Einträge in anderen Dateien automatisch durchgeführt werden.

Sie können nun den `named` starten durch Eingabe von **`named [↵].`**



| |
|---|
| **Tip:** Beobachten Sie in einem anderen Xterminal bzw. auf einer anderen Konsole die Datei `/var/log/messages`. Jede Änderung können Sie sich anzeigen lassen, indem Sie eingeben: **tail –f /var/log/messsages [↵]** |

## 4) Testen der Konfiguration

a) Auf Ihrem Linux-Server können Sie die korrekte Namensauflösung mit dem Befehl **`nslookup`** `testen`. Geben Sie einen DNS-Namen ein und Ihr Server antwortet mit der zugehörigen IP-Adresse. Die Ausgabe sieht ungefähr wie folgt aus:

```
test@server1:/home/test > nslookup
Default Server:  server1
Address:  0.0.0.0

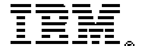
> www.vivex.de
Server:  server1
Address:  0.0.0.0

Non-authoritative answer:
Name:    www.vivex.de
Address:  195.122.135.172
```

Sie können nslookup mit [Strg]+[C] beenden.

b) Auf Ihrer Workstation können Sie einer MS-DOS-Eingabeaufforderung ping-Kommandos absetzen und als Zieladresse Rechnernamen verwenden. Beispiel:

**ping www.vivex.de [↵]**



---

 **Übung 7-1:** Einrichten eines DNS-Cache-Servers

---

## 7.3 * Einrichtung eines vollwertigen DNS-Servers *(optional)*

Wenn die Namen aller Arbeitsstationen des lokalen Netzes im DNS bekannt sein sollen, müssen Sie einen eigenen "vollwertigen" Name-Server einrichten. Der Name-Server, den unser DNS-Cache-Server befragt (BelWü), kennt diese Namen nämlich nicht. Da Sie die Namen der lokalen Arbeitsstationen jedoch zu keinem Zeitpunkt benötigen und die Einrichtung eines DNS-Servers sehr fehlerträchtig ist, ist dieses Kapitel optional.

Wie im Kapitel 7.1 d) erwähnt, benötigt ein Name-Server vier Dateien, die hier `named.local`, `named.hosts`, `named.rev` und `root.cache` genannt werden[11] und als *DNS-Datenbankdateien* bezeichnet werden sollen. Diese werden sinnvollerweise alle im Verzeichnis `/var/named` abgelegt, welches bereits existiert und die Datei `root.cache` enthält. Zunächst einige Erläuterungen zu diesen DNS-Datenbankdateien:

### 7.3.1 Die DNS-Datenbankdateien

Alle vom *named* verwendeten DNS-Datenbankdateien beziehen sich auf eine Domäne, welche als *origin* bezeichnet wird. Der zugehörige Domänenname wird in der Datei `/etc/named.boot` hinter den `cache` und `primary`-Kommandos angegeben. Innerhalb einer Datenbankdatei können Domänen- und Rechnernamen *relativ* zu dieser Domäne (origin) festgelegt werden. Wenn ein Name *absolut* angegeben werden soll, muss er mit einem einfachen Punkt beendet werden. Anstelle des vollständigen *origin*-Namens darf in den DNS-Datenbankdateien auch das Zeichen @ verwendet werden.

In den DNS-Datenbankdateien können nun z.B. die Namen der Name-Server einer Domäne, Abbildungen von Rechnernamen auf IP-Adressen (Rechnerdatei) oder Abbildungen von IP-Adressen auf Rechnernamen (umgekehrte Rechnerdatei) aufgeführt werden. Alle DNS-Datenbankdateien haben eine ähnliche Grundstruktur und setzen sich aus Einträgen

---

[11] Die Namen sind frei wählbar und werden in der Datei `/etc/named.boot` festgelegt.





einer einzigen Art, den sog. Standard **R**esource **R**ecords (**RR**) zusammen. Diese bilden die kleinste Informationseinheit, die im DNS verfügbar ist und bei Namensanfragen ausgetauscht wird. Jeder RR hat folgendes Format:

*[Name]* *[ttl]* *Klasse* *RR-Typ* *typspezifische Daten*

Dabei bedeuten:

### Name

Name eines Domänenobjekts auf den sich der RR bezieht. Ein Domänenobjekt kann ein Rechner oder auch eine vollständige Domäne sein. Steht ein Leerzeichen statt *Name*, so bezieht sich der Eintrag auf das zuletzt in der Datei benannte Domänenobjekt. Weitere Sonderzeichen für *Name* sind:

**.** : Der Punkt bezeichnet die root-Domäne

@ : Bezeichnet den aktuellen Domänennamen, gemäß der mit dem Namen der DNS-Datenbankdatei korrespondierenden *primary*-Direktive in der `/etc/named.boot`

**;** : Leitet einen Kommentar ein, der mit [↵] beendet wird

### ttl (Time To Live)

Gibt an, wie lange die Daten im Cache gültig bleiben. Nach Ablauf dieser Zeit (in Sekunden) müssen Informationen erneut vom Name-Server angefordert werden. Hierdurch wird erreicht, dass ein Name-Server auf Änderungen von Domänennamen reagieren kann. Wird keine Zeit angegeben, so wird der Wert des *minimum*-Feldes des vorausgehenden (einleitenden) *SOA-records* verwendet (siehe hinten!).

### Klasse

Hat stets den Wert IN (= TCP/IP). Weitere Klassen gibt es zur Zeit nicht.

### RR-Typ

Definiert den Typ und somit die Funktion des RRs. Die wichtigsten Funktionen sind:

- SOA : (**S**tart **o**f **A**uthority) definiert die Domäne, auf die sich alle folgenden RRs beziehen
- NS : definiert einen **Name-Server**
- A : bildet Rechnernamen auf IP-**A**dressen ab
- CNAME : (**C**anonical Host**name**) bildet Rechnernamen auf Alias-Namen ab
- PTR : bildet IP-Adresse auf Rechnernamen ab
- MX : (**M**ail E**x**changer) definiert einen Mailhost der betreffenden Domäne

Für eine vollständige und ausführliche Beschreibung der Funktionen sei auf die Dokumentation der jeweiligen *bind*-Software bzw. auf die entsprechende Literatur verwiesen.








### 7.3.2 Editieren der Ladedatei `/etc/named.boot`

Mit Hilfe dieser Datei wird der Namens-Dämon *named* konfiguriert. Sie haben für den DNS-Cache-Server bereits in Kap. 7.2 2) einige Einträge kennengelernt. Nun muss die Datei um folgende (hier fett gedruckte) Einträge erweitert werden:

```
directory   /var/named

primary     0.0.127.in-addr.arpa         named.local
primary     schule1.alf.es.bw.schule.de  named.hosts
primary     0.0.10.in-addr.arpa          named.rev

cache       .                            root.cache
forwarders  129.143.2.4
slave
```

Der erste `primary`-Eintrag gibt an, dass der *named* als primärer Name-Server für das Loopback-Netz arbeitet und die zugehörigen Daten in der Datei `named.local` zu finden sind. Sie müssen beachten, dass in diesem Fall die Netzwerkadresse (bis auf das letzte Segment) rückwärts zu schreiben und der Begriff `in-addr.arpa` anzuhängen ist. Dieser Begriff steht für eine Pseudo-Domain, die für das *Reverse Mapping* verwendet wird.

Mit dem zweiten `primary`-Eintrag wird der *named* angewiesen, die Domain `schule1.alf.es.bw.schule.de` als primärer Name-Server zu verwalten. Die dazugehörigen Verwaltungsdaten sind aus der Datei `named.hosts` zu lesen.

Der dritte `primary`-Eintrag weist den *named* an, die Rückwärtsabbildung der zu der angegebenen Domain gehörenden IP-Adressen als primärer Name-Server zu verwalten.

Alle weiteren Einträge wurden bereits im Kapitel 7.2 besprochen.

### 7.3.3 Anlegen der Datei `/var/named/named.local`

Zunächst soll die Namensauflösung für das Localhost-Netz konfiguriert werden. Hierfür ist die Datei `/var/named.local` zuständig. Diese ist noch nicht vorhanden und muss manuell angelegt werden.






Nachfolgend ein Beispiel:

```
;
; /var/named/named.local
;
@   IN   SOA   server.schule1.alf.es.bw.schule.de.
root.schule1.alf.es.bw.schule.de.   (
              1998060801                 ; Seriennr.
              360000                     ; Refresh: 100 Stunden
              3600                       ; Wiederholung: 1 Stunde
              3628800                    ; Ablauf: 42 Tage
              360000                     ; Minimum: 100 Stunden
              )

    IN   NS    server.schule1.alf.es.bw.schule.de.
1   IN   PTR   localhost.
```

**Achtung:** Die Einträge in der vierten und fünften Zeile gehören eigentlich in eine Zeile und sind nicht durch ein [↵] voneinander getrennt; der Zeilenumbruch ist in dieser Unterlage nur wegen der geringen Seitenbreite entstanden!

Nach den Kommentaren erkennen Sie in der ersten Zeile die Sytntax für einen RR, lediglich die typspezifischen Daten seien kurz erläutert:

- Hier wird ein RR vom Typ *SOA* definiert.
- Erstes Argument der typspezifischen Daten ist der vollständige DNS-Name des Namservers `server.schule1.alf.es.bw.schule.de.`, welcher als absolut zu betrachten ist, da er mit einem Punkt abgeschlossen ist.
- Zweites Argument ist die Postadresse des verwaltenden Benutzers `root.schule1.alf.es.bw.schule.de.`, wobei hier im Gegensatz zu einer E-Mail-Adresse anstelle des @-Zeichens hinter dem Benutzernamen ein Punkt verwendet wird.
- Drittes Argument ist eine durch runde Klammern () eingeschlossene Folge von Zahlen mit folgender Bedeutung:
  Die erste Zahl steht für eine Seriennummer, die zwar eindeutig sein muss, aber selbst definiert werden kann. Überlicherweise wird das Erstellungsdatum und eine laufende Nummer gewählt. Jede Datenbankdatei muss eine andere Seriennummer enthalten! Die Seriennummer stellt beim Abgleich mit einem Secondary-Name-Server das Abgleichkriterium dar. Die Angaben für die Refresh-Zeiten und andere Zeiten sind in Sekunden anzugeben.

Anschließend folgen zwei weitere RRs, die den Namen des eigenen Rechners festlegen.



### 7.3.4 Anlegen der Datei `/var/named/named.hosts`

Als nächstes legen Sie die Rechnerdatei `/var/named.hosts` an, die die Zuordnung von Namen zu IP-Adressen ermöglicht. Hierfür enthält die Datei für jeden Rechner in Ihrer Domäne wenigstens einen RR vom Typ A (Name → IP-Adresse). Optional können Sie sog. Aliasnamen eintragen, damit beispielsweise der Rechner 'server' auch unter dem Namen 'www' angesprochen werden kann. Aliasnamen werden in RRs vom Typ CNAME festgelegt. Die Rechnerdatei könnte dann wie folgt aussehen:

```
;
; /var/named/named.hosts
;
@      IN    SOA   server.schule1.alf.es.bw.schule.de.
root.schule1.alf.es.bw.schule.de.   (
                        1998060802        ; Seriennr.
                        86400             ; Refresh: 1mal am Tag
                        3600              ; Wiederholung: 1 Stunde
                        3628800           ; Ablauf: 42 Tage
                        604800            ; Minimum: 1 Woche
                        )
      IN    NS    server.schule1.alf.es.bw.schule.de.
      IN    MX    10    server

;loopback
localhost.  IN    A     127.0.0.1

server      IN    A     10.0.0.1
Mail-Server IN    A     10.0.0.1
ws01        IN    A     10.0.0.11
ws02        IN    A     10.0.0.12
idefix      IN    A     10.0.0.102

www         IN    CNAME server.schule1.alf.es.bw.schule.de.
; hier koennte ebenso stehen:
; www       IN    CNAME server

FTP         IN    CNAME server.schule1.alf.es.bw.schule.de.
news        IN    CNAME server

all         IN    A     255.255.255.255
```

**Achtung:** Die Einträge in der vierten und fünften Zeile gehören eigentlich in eine Zeile und sind nicht durch ein [↵] voneinander getrennt; der Zeilenumbruch ist in dieser Unterlage nur wegen der geringen Seitenbreite entstanden!

Die Syntax von RRs ist Ihnen mittlerweile bekannt. Nachfolgend folgende Hinweise:

- Der Eintrag "`IN MX 10 server`": Da kein "Name" angegeben ist, bezieht sich der Eintrag auf die zuletzt genannte Domäne `schule1.alf.es.bw.schule.de`. Der RR besitzt die Klasse TCP/IP (`IN`) und ist vom Typ Mail Exchanger (`MX`). Hierduch wird also der lokale Mail-Server der Domäne spezifiziert. Das erste Argument (`10`) gibt die Priorität des Mail-Servers an (1: groß ... 10: klein) und ist nur von Bedeutung, wenn mehrere Mail-Server existieren. Das zweite Argument (`server`) ist der Name des Mail-Servers.
- In den nachfolgenden Zeilen werden schließlich die Namen der Rechner in der eigenen Domäne aufgeführt. Die RRs sind vom Typ `A` (Zuordnung Name → IP-Adresse) oder `CNAME` (Aliasname)

### 7.3.5 Anlegen der Datei `/var/named/named.rev`

Abschließend legen Sie die umgekehrte Rechnerdatei an, die die Zuordnung IP-Adresse → Name ermöglicht. Diese könnte wie folgt aussehen:

```
;
; /var/named/named.rev
;
@      IN     SOA   server.schule1.alf.es.bw.schule.de.
root.schule1.alf.es.bw.schule.de.         (
                        1998060803  ; Seriennr.
                        86400       ; Refresh: 1mal am Tag
                        3600        ; Wiederholung: 1 Stunde
                        3628800     ; Ablauf: 42 Tage
                        604800      ; Minimum: 1 Woche
                  )

      IN     NS     server.schule1.alf.es.bw.schule.de.

1.1   IN     PTR    server.schule1.alf.es.bw.schule.de.
11.1  IN     PTR    ws01.schule1.alf.es.bw.schule.de.
12.1  IN     PTR    ws02.schule1.alf.es.bw.schule.de.
102.1 IN     PTR    idefix.schule1.alf.es.bw.schule.de.
```

Zu beachten ist bei der umgekehrten Rechnerdatei, dass die RRs vom Typ `PTR` (Zuordnung IP-Adresse → Name) sind und dass die IP-Adressen **rückwärts** geschrieben werden. Hierbei geben Sie nur diejenigen Bytes an, die kombiniert mit den zugehörigen Bytes der betreffenden `primary`-Direktive in der Datei `/etc/named.boot` für die Angabe einer vollständigen (umgekehrten) IP-Adresse fehlen (`primary` **`30.172.`**`in-addr.arpa named.rev`).





# 8 Proxy

Wenn viele Clients dieselben Internet-Dokumente abrufen, lässt sich die Zugriffszeit erheblich verkürzen, wenn die Dokumente nach dem ersten Zugriff auf einem Server im lokalen Netz zwischengespeichert werden. Hierfür dient der Kommunikationsserver als *Proxy* [12].

**Ziele dieses Kapitels:**

1. Beschreiben der Funktionalität eines Proxyservers
2. Konfigurieren des "Squid"-Proxys

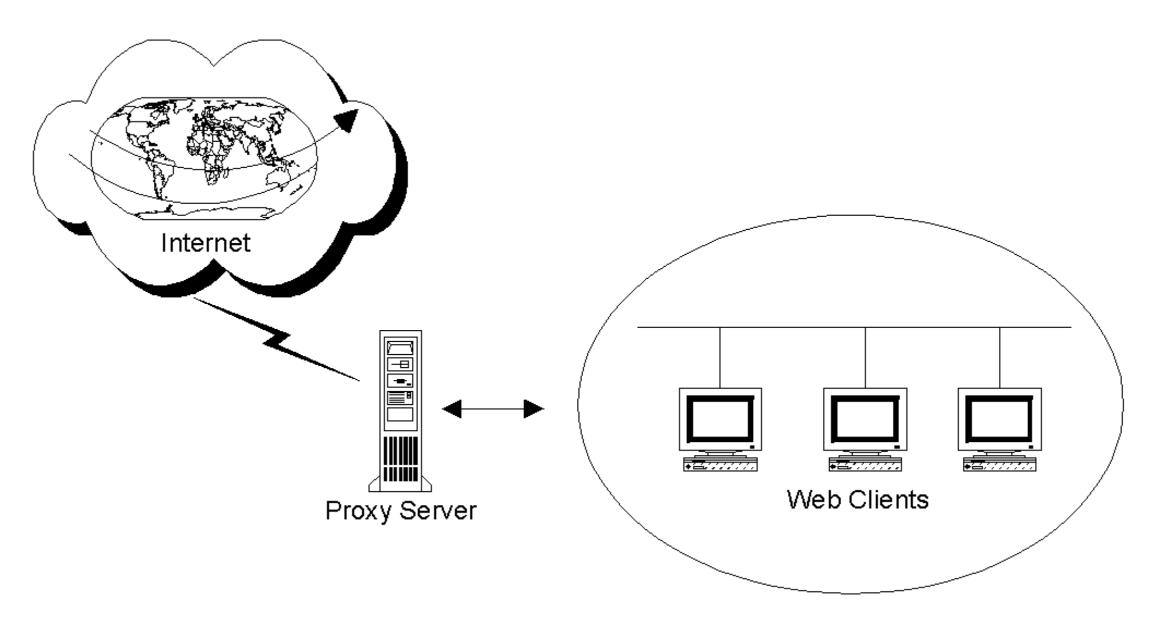
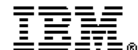



**Abbildung 8-1:** Einsatz des Linux-Servers als Proxy-Server

## 8.1 Funktionsweise eines Proxy-Servers

Durch Verwendung eines Proxy-Zwischenspeichers (Cache) in Ihrem LAN können Sie den Zugriff auf Informationen im Internet erheblich beschleunigen. Alle abgerufenen Informationen werden lokal auf dem Proxy gespeichert, so dass bei erneuten Anfragen kein Zugriff ins Internet mehr erforderlich ist, sondern aus dem lokalen Proxy-Cache bereitgestellt werden. Damit reduzieren sich auch die Kosten für den Internetzugang, da die Verbindung zum Provider nur für nicht zwischengespeicherte Informationen benötigt wird.

[12] Proxy: Zwischenspeicher für Internet-Dokumente



Wenn sie Ihren Proxy aktiviert haben, werden die Internet-Anfragen Ihrer Clients zuerst an den Proxy-Server geleitet. Dieser sucht die angeforderte Information in seinem Cache. Nur wenn sich die benötigten Informationen nicht im Proxy-Cache befinden, fordert der Proxy sie beim vom Client angegebenen Ziel an, speichert sie in seinem Cache und stellt Sie dem Client zur Verfügung.

Sämtliche Anfragen ins Internet werden somit nicht mehr direkt von verschiedenen Clients, sondern von einem Proxy-Server gestellt. Er bietet damit automatisch eine Zugangskontrolle zum Internet.

Die meisten WWW-Browser verwenden unabhängig von einem evtl. vorhandenen Proxy-Server zusätzlich einen lokalen Cache. Dieser kann und sollte deaktiviert werden, wenn über einen Proxy-Server ins Internet zugegriffen wird.

## 8.2 Grundlagen des Squid-Proxys

In der S.u.S.E.-Distribution ist die Proxy-Software SQUID enthalten und bereits installiert, wenn Sie während der Linux-Installation die Konfiguration *Internet access server* ausgewählt haben[13].

Wenn Sie aus dem Internet Informationen abrufen, wird auf dem Weg zur Quelle dieser Informationen i.d.R. wenigstens ein weiterer Proxy-Server liegen. So verwenden beispielsweise viele Provider einen Proxy-Server. (**Achtung:** BelWü verwendet *keinen* eigenen Proxy, jedoch steht i.d.R. der Proxy der nächsten Hochschule/Universität zur Verfügung.)

Abhängig von der Anordnung dieser Proxys ergibt sich eine Cache-Hierarchie. Wenn Ihr Proxy neue Informationen nur von einem übergeordneten Proxy bezieht (z.B. vom Provider), dann ist der übergeordnete Proxy ein sog. *Parent-Cache*. Proxys, die auf derselben Ebene der Cache-Hierarchie liegen, heißen *Neighbour-Cache*. Ein solcher Neighbour-Cache könnte beispielsweise der Proxy einer anderen Schule sein, der über denselben Provider ans Internet angebunden ist.

Der wesentliche Unterschied zwischen den beiden Cachetypen liegt im Verhalten beim Beschaffen von Webseiten, die noch nicht im lokalen Cache liegen. Wird die Anfrage für eine solche Seite an einen *Parent-Cache* gestellt, so wird davon ausgegangen, dass dieser die Seite beim Quell-Web-Server beschafft. Bei einem *Neighbour-Cache* wird in einem solchen Fall der Quell-Web-Server selbst angefragt.

Bei der Konfiguration des *squid* können zum Einbinden in eine Cache-Hierarchie die Parent- oder Neighbour-Caches angegeben werden. Zu beachten ist, dass beim *squid* der Begriff „sibling“ anstelle von „neighbour“ verwendet wird.


[13] Alternativ finden Sie das Paket *squid* in der Serie **n**.

Wenn Sie beabsichtigen, einen solchen Cache-Verbund einzurichten, so ist für die Nutzung von fremden Proxys natürlich grundsätzlich vorher das Einverständnis des Betreibers einzuholen.

Die **Konfiguration** des Proxys *squid* erfolgt im wesentlichen über die Datei:

`/etc/squid.conf`.

Im folgenden werden nur die wichtigsten Parameter dieser Konfigurationsdatei erläutert, da eine vollständige Beschreibung im Rahmen dieser Kursunterlage nicht möglich ist. Stattdessen sei auf die zugehörige **Dokumentation** verweisen, die Sie unter

`/usr/doc/packages/squid`

vorfinden. Eine Manual-Page zu squid ist leider noch nicht verfügbar. In der Konfigurationsdatei `/etc/squid.conf` sind jedoch viele Kommentare enthalten, die Ihnen weiterhelfen können. Auf der Squid-Homepage

`http://squid.nlanr.net`

finden Sie weitere Hinweise sowie eine FAQ.

## 8.3 Die Konfigurationsdatei `/etc/squid.conf`

Die Datei `squid.conf` ist in verschiedene Sektionen unterteilt, von denen hier die Themen: (a) Einbinden in einen Cache-Verbund, (b) Definition der Cache-Parameter sowie (c) Zugangskontrolle zu einem Proxy behandelt werden. Ferner werden einige weitere ausgesuchte Einträge besprochen, die für den Betrieb des Proxys wichtig sind.

### 8.3.1 Port-Nummern

Gleich zu Beginn der Datei `squid.conf` befinden sich die Einträge für die verwendeten Ports:

```
http_port 3128
icp_port 3130
```

Mit dem ersten Eintrag wird der Port festgelegt, auf dem der Proxy Anfragen von WWW-Clients erwartet. Der zweite Eintrag legt die Port-Nummer fest, die für ICP-Anfragen benutzt wird. Die gezeigten Werte sind die Default-Einstellungen, die auch ohne explizite Angabe von Port-Nummern verwendet werden.

***Achtung:*** *Die meisten Web-Browser verwenden als Standard-Port für Proxy-Anfragen den Port 80. Sie müssen demzufolge auf den Client-PC's im jeweiligen Web-Browser die IP-Adresse Ihres Proxys (=Linux-Server) und die Portnummer '3128' eintragen, damit Ihr Proxy verwendet werden kann!*

### 8.3.2 Verantwortlicher für den Proxy

Hinter dem Schlüsselwort `cache_mgr` sollten Sie unbedingt die E-Mail-Adresse des für den Proxy Verantwortlichen eintragen:

```
cache_mgr  webmaster@schule1.alf.es.bw.schule.de
```

### 8.3.3 Benutzerkennung für den squid

Aus Sicherheitsgründen sollte squid nie mit Root-Rechten laufen. Falls dies aber beim Starten unumgänglich ist, kann mit diesem Eintrag erreicht werden, dass squid mit den Rechten des hier angegebenen Users läuft. Die gezeigte Vorgabe ist bei S.u.S.E. schon voreingestellt:

```
cache_effective_user squid nogroup
```

### 8.3.4 Name des Proxyservers

Wenn Sie einen bestimmten Namen, sowie verschiedene Systemmeldungen anstelle des vom System gelieferten Namens in Logfiles angezeigt bekommen möchten, so müssen Sie diesen Namen hier angeben:

```
visible_hostname www.schule1.alf.es.bw.schule.de
```

Alle bisher und später nicht explizit angesprochenen Einträge kann man für normale Anforderungen unverändert lassen.

### 8.3.5 Logdateien

Log-Dateien werden per *default* im Verzeichnis:

```
/var/squid/logs
```

abgelegt.

Sie finden dort die Dateien:

| | |
|---|---|
| `access.log` | Logdatei für Client-Anfragen. Enthält einen Eintrag für jede HTTP- und ICP-Anfrage |
| `cache.log` | Logdatei über den Zustand des Cache und alle Cache-Aktivitäten |
| `store.log` | Logdatei über gespeicherte Objekte, Speicherdauer und Zugriff auf diese Objekte |

Wenn Sie den Speicherort bzw. Optionen für die Logdateien ändern wollen, editieren Sie die gleichnamigen Abschnitte der Datei `/etc/squid.conf` .

Sinnvoll ist ferner folgender Eintrag:

```
emulate_httpd_log on
```

Hierdurch werden u.a. in den Logdateien Zugriffsdatum und –zeit im Klartext abgespeichert.

### 8.3.5 * Einbinden in einen Cache-Verbund *(optional)*

Wenn Ihr Provider ebenfalls einen Proxy verwendet, können Sie diesen als *Parent-Cache* eintragen. Da BelWü **keinen** eigenen Proxy benutzt, ist das folgende Kapitel 8.3.5 für Sie zunächst ohne Bedeutung! Sie können jedoch ggf. den Proxy der nächsten Hochschule/Universität als Parent-Cache verwenden, wenn Sie dies telefonisch mit BelWü und der Hochschule/Universität absprechen.

Der für einen Cache-Verbund wichtige Punkt ist der `cache_host`-Eintrag. Mit diesem Schlüsselwort werden Neighbour- und Parent-Caches definiert. Der Aufbau einer Zeile für einen solchen Eintrag sieht folgendermaßen aus:

```
cache_host type http_port icp_port options
```

Für die einzelnen Spalten sind folgende Einträge möglich:

| | |
|---|---|
| `type` | parent, sibling, multicast |
| `http-port` | Nummer des Ports, an dem squid auf Anfragen von WWW-Clients warten soll |
| `icp-port` | Nummer des Ports, auf dem squid auf ICP-Messages wartet. Für die Verbindung mit Proxys ohne ICP-Support ist dort „7“ anzugeben. Da- |

bei ist zu beachten, dass das andere System auch „echo requests“ antworten muss.

`options` Die wichtigsten Angaben hier sind „proxy-only“, „weight“, „no-query“ und „round-robin“. Durch die Angabe von „proxy-only wird erreicht, dass die vom angefragten Proxy gelieferten Daten nicht im lokalen Cache gehalten werden. Mit „weight“ kann man eine Gewichtung bei der Angabe von mehreren Parent-Caches erreichen. Die Angabe erfolgt als ganze Zahl und per default ist „1“ eingestellt. Größere Werte bewirken eine Bevorzugung des angegebenen Proxys. Die Angabe von „no-querys“ bewirkt, dass an den angegebenen Proxys keine ICP-Anfragen geschickt werden. Mit der Option „round-robin“ kann eine Liste von Proxys angegeben werden, die im Round-Robin-Verfahren angesprochen werden. Sinn einer solchen Maßnahme ist gewöhnlich eine Lastverteilung auf mehrere Systeme.

Nachfolgend ein **Beispiel**.:

Die Firma Vivex GmbH verwendet in Ihrem internen Netz nichtroutbare IP-Adressen 10.0.0.X, außerdem einen Proxy (Novell™ BorderManager™) mit der IP-Adresse 10.0.0.103. Dieser Proxy arbeitet auf dem Port 8080 und verwendet für ICP-Anfragen den Standard-Port 3130. Wenn wir diesen Proxy als Parent-Cache verwenden wollen, so lautet der korrekte Eintrag:

```
cache_host 10.0.0.103 parent 8080 3130
```

Für das Beispiel ist der Vivex-Proxy als sog. Parent-Cache definiert. Das bedeutet, dass alle Anfragen von unserem eigenen Proxy an diesen Proxy weitergeleitet werden. Ist das gewünschte Dokument nicht im dortigen Cache vorhanden, so ist es Aufgabe des Vivex-Proxys, dieses zu beschaffen. Unser eigener Proxy wartet jedenfalls, bis die Anfrage von dort beantwortet wird oder eine Ablehnung erfolgt.

Wäre der Vivex-Proxy als „sibling“ definiert, so käme von dort per ICP die Nachricht, dass das gewünschte Dokument nicht verfügbar ist. Danach würde unser Proxy das Dokument selbst beim zuständigen WWW-Server beschaffen. An dieser Stelle ist eine Vielzahl von Kombinationen möglich, die man jeweils den spezifischen Bedingungen entsprechend zusammenstellen muss.

Für die Nutzung eines Proxys, der kein ICP beherrscht, wie zum Beispiel der Netscape-Proxy-Server, muss man folgenden Eintrag verwenden:

```
cache_host proxy.provider.de parent 3128  7  no-query default
```

Für diesen speziellen Fall kann nur der Typ *parent* verwendet werden. Der ICP-Port muss mit „7“ besetzt werden, die Option „no-query“ muss angegeben werden.

Mit der folgenden Angabe kann man erreichen, dass für bestimmte Domains nur ausgewählte Proxy-Rechner angesprochen werden.

```
cache_host_Domain cache-host domain [domain...]
```

In Spalte zwei steht der Proxy-Rechner, auf den sich der Eintrag bezieht. Danach folgt eine Liste von Domänen, für die der Proxy auf dieser Maschine angesprochen wird. Durch Voranstellen eines „!“ kann eine negierende Wirkung erzielt werden. Damit ist gemeint, dass für die angegebene Domain dieser Proxy *nicht* angesprochen wird.

```
local_domain planet.de
```

Durch die Angabe dieses Parameters wird squid angewiesen, alle Anfragen an Rechner innerhalb dieser Domain direkt auszuführen und keinen *Neighbour-* und *Parent-Cache* anzufragen. Auch die Auflistung von weiteren Domains ist, durch Leerzeichen getrennt, möglich.

```
FTP_user  squid@venus.planet.de
```

Dieser Wert ist per Voreinstellung auf „squid@“ eingestellt. Wir sollten hinter dem Zeichen „@“ noch unseren Rechnernamen einschließlich Domain-Bezeichnung angeben. Ohne diese Angabe kann es beim Download auf einigen FTP-Servern Probleme geben.

### 8.3.6 * Festlegen der Cacheparameter *(optional)*

Squid benutzt ein doppeltes Cachesystem, d.h. Daten werden zum einen im Speicher (RAM) und zum anderen auf der Festplatte gehalten. Die Größe dieser Caches lässt sich festlegen. Für den Speichercache (virtual memory) ist folgender Eintrag zuständig:

```
cache_mem 16
```

Durch diese Angabe wird eine Cachegröße von 16 Mbyte definiert. Ohne Angabe verwendet Squid einen Cache von 8 Mbyte. Dieser wird ähnlich wie ein Ringpuffer verwaltet. Man sollte diesen Cache zur Steigerung der Performance möglichst groß (ca. ¼ RAM) wählen.

Neben der Festlegung der Größe gibt es noch zwei weitere Parameter, die auf die Verwaltung des Caches Einfluss nehmen. Diese sind `cache_mem_low` und `cache_mem_high`. Diese Variablen sind auf 75% und 90% voreingestellt. Normalerweise kann man diese Werte so belassen. Sie definieren die Grenzwerte, zwischen denen der Füllungsgrad des Caches gehalten wird. Bei Überschreitung von 90% werden weniger häufig benötigte URLs aus dem Cache entfernt, bis die Auslastung des Caches wieder auf 75% abgesunken ist.

```
cache_swap 200
```

Mit dieser Angabe wird die Größe des oben erwähnten Festplatten-Caches auf 200 Mbyte festgelegt. Die Standardeinstellung für diesen Wert ist 100 Mbyte. Wenn Sie über genügend Platz auf Ihrer Festplatte verfügen, sollte diesen Wert ruhig vergrößert werden (200 MB sollten ausreichen). Auch hier gibt es wieder zwei Grenzwerte für den Füllungsgrad, für die die gleichen Aussagen wie für `cache_mem` gelten.

---



**Übung 8-1:** Grundkonfiguration des Proxys squid

---

### 8.3.7 Zugriffsregeln für den Squid-Proxy

Bisher sind Ihre Clients in der Lage, beliebige Informationen aus dem Internet anzufordern. Dies ist für bestimmte Informationen rechtlich und moralisch bedenklich, wenn beispielswei-

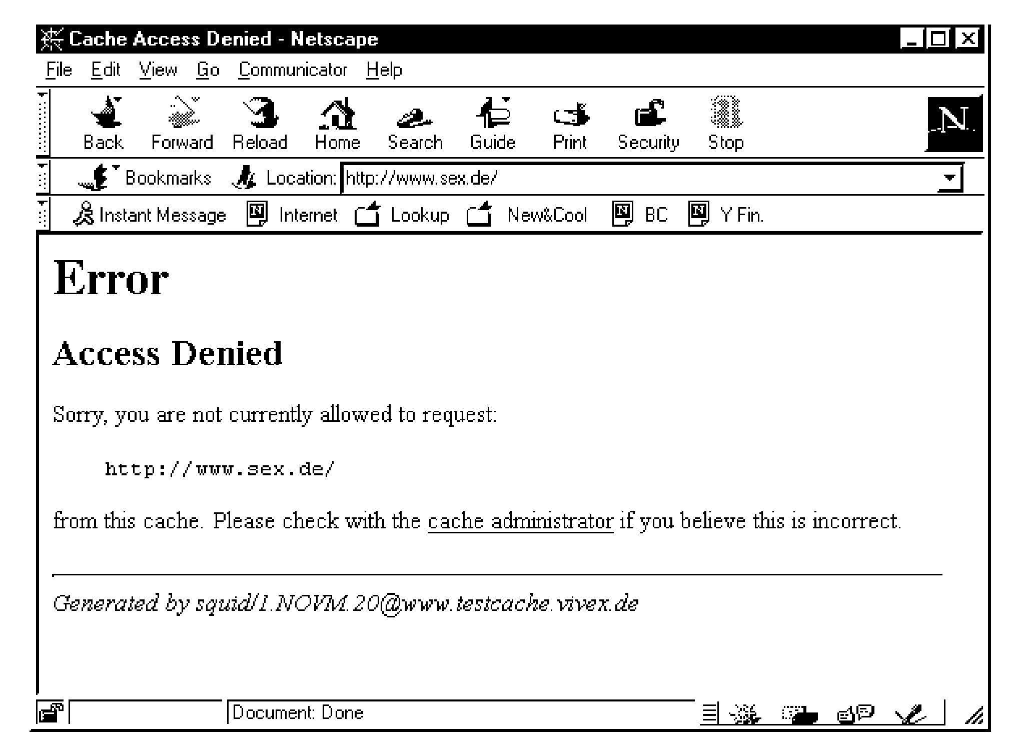



**Abbildung 8-2:** Zugangskontrolle auf Webseiten mit dem Proxy *squid*

se Minderjährige Webseiten mit pornographischem Inhalt aufrufen
Der Proxy-Squid bietet Ihnen die Möglichkeit, den Zugriff auf Internet-Informationen zu kontrollieren und zu reglementieren. Dies geschieht über die Definition von Zugangs-Kontroll-Listen (englisch: ***A****ccess* ***C****ontrol* ***L****ist*), die eine Menge von Computern, Domänen etc. zusammenfassen, für die eine Reglementierung gelten soll. Für diese ACL kann dann der Zugriff gestattet bzw. verwehrt werden,

Mit Hilfe der ACLs ist es auf sehr vielfältige Art und Weise möglich, den Zugriff auf den Proxy einzuschränken. Dabei können einzelne IP-Adressen oder ganze Bereiche genauso wie Domains oder Protokolle und Portnummern als Kriterien herangezogen werden. Auch zeitliche Einschränkungen oder das Überprüfen von Zeichenketten in kompletten URLs oder im URL-Pfad sind möglich.

## Prinzipielles Verfahren

1. Jede ACL bekommt einen **Namen** (`aclname`). Verwenden Sie möglichst Namen, die die Aufgabe der ACL verdeutlichen, z.B. *local* für alle Rechner im lokalen Netz.

2. Jede ACL ist von einem bestimmten **Typ** (`acltype`). Sie definieren hier, ob Sie eine Regel für bestimmte IP-Adressen (im lokalen oder im Zielnetz), Domänen-Namen, Zeichenketten oder Internet-Protokolle aufstellen.

3. Je nach Typ benötigt eine ACL **Argumente** (`string`). Wenn Sie bspw. eine Regel vom Typ *IP-Adresse* definieren, folgen als Argumente alle IP-Adressen, für die die Regel gelten soll.

4. Abschließend legen Sie fest, ob für die betreffende ACL der Zugriff **erlaubt** (`allow`) oder **verboten** (`deny`) ist.

**Hinweise:** Wenn Sie für eine ACL mehrere Argumente (z.B. IP-Adressen) angeben, dann werden diese logisch ODER-verknüpft. Bei mehreren IP-Adressen bedeutet das z.B., dass die Regel für die erste, oder die zweite, oder die dritte oder auch alle IP-Adressen gilt.

Auf die definierten ACLs wird zum Erlauben bzw. Verbieten mit `http_access`- oder `icp_access`-Einträgen Bezug genommen. In beiden Fällen können mehrere ACLs als Parametern angegeben werden. Dort werden dann alle Elemente logisch UND-verknüpft. Wenn z.B eine Erlaubnis `http_acces allow` für die ACLs `local01` und `local02` definiert wird, dann gilt sie für alle Elemente in der ACL `local01` und `local02`.






## Aufbau einer Zugangsregel

Eine Zugangsregel wird immer nach folgenden Schema aufgebaut:

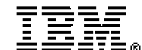
| | | | |
|---|---|---|---|
| acl | aclname | acltype | string [string2...] |
| http_access | allow\|deny | [!]aclname | |
| icp_access | allow\|deny | [!]aclname | |

Die **erste Zeile** zeigt dabei den Aufbau eines ACL-Eintrages:

- Der Eintrag beginnt immer mit dem Schlüsselwort **acl**.
- Jede ACL erhält im Feld **aclname** einen eindeutigen, frei wählbaren Namen. Dieser sollte die Aufgabe der ACL verdeutlichen.
- Im Feld **acltype** wird der Typ der ACL festgelegt. Mögliche Typen sind:

| | |
|---|---|
| `src (Quelle)` | IP-Adresse eines Clients in der Form Adresse/Netmask. Möglich ist auch die Angabe eines Adressbereiches, wobei Anfangs- und Endadresse mit einem „-„ getrennt sein müssen. |
| `dst (Ziel)` | Gleiche Syntax wie bei „src“, aber die Adresse des Ziel-Rechners im Internet ist relevant. |
| `srcdomain` | Angabe einer Domain als Quelle. |
| `dstdomain` | Angabe einer Domain als Zieldomain. |
| `url_regex` | Ein String, der auch Wildcards enthalten kann, wird mit dem Inhalt der kompletten URL verglichen. |
| `urlpath_regex` | Ein String mit Wildcards wird mit dem URL-Pfad verglichen. |
| `proto` | Angabe eines Protokolls wie HTTP oder FTP usw. |
| `port` | Angabe einer Portnummer. |
| `time` | Abkürzungen für Wochentage, Zeitbereiche im Format h1:m1-h2:m2 |
| `user` | Benutzername |
| `method` | Zugriffsmethode wie GET oder POST (wird zum Ausfüllen von Formularen bzw. in Suchmaschinen verwendet). |

- Im Feld **string** [string2,...] werden die Argumente angegeben, die je nach ACL-Typ benötigt werden (z.B. IP-Adressen). Diese Angaben werden nacheinander, durch Leerzeichen getrennt, aufgelistet. Alternativ kann man, in Anführungszeichen gesetzt, einen Dateinamen angeben, der die entsprechenden Informationen enthält. In dieser Datei darf in jeder Zeile nur jeweils ein Eintrag stehen.



Die **zweite und dritte Zeile** zeigen den Aufbau einer Zugangserlaubnis bzw. –verweigerung.

- Eine Zugangserlaubnis bzw. –verweigerung beginnt immer mit dem Schlüsselwort

  `http_access` für Regeln, die sich auf das http-Protokoll beziehen; das ist der Normalfall, bzw.:

  `icp_access` für Regeln, die sich auf das icp-Protokoll (Kommunikation zwischen Proxys) beziehen; das ist eher die Ausnahme.

- Es folgt die Aktion

  `allow` Zugang gestatten, bzw.:

  `deny` Zugang abweisen.

- Abschließend wird der Name der betreffenden ACL(s) eingetragen. Werden mehrere ACLs angegeben, so werden diese UND-verknüpft.

## Default-Regeln

Die Datei `squid.conf` enthält per default folgende Zugriffsregeln:

```
acl localhost src 127.0.0.1/255.255.255.255
acl manager Proto cach_object
acl all src 0.0.0.0/0.0.0.0
acl SSL_ports port 443 563
acl CONNECT method CONNECT
# Allow everything else
http_access deny manager!localhost
http_access deny CONNECT !SSL_ports
http_access allow all
# Reply to all ICP queries we receive
icp_access allow all
```

Zu Beginn werden fünf ACLs mit den Namen „localhost“, „manager“, „all“, „SSL-Ports“ sowie „CONNECT“ definiert. Auf diese wird in den nachfolgenden Zeilen Bezug genommen.

- Der erste davon weist für Access-Liste „Manager“ nur den Rechner localhost nicht ab.
- Beim zweiten wird der HTTP-Zugang abgewiesen für die Methode CONNECT auf andere als den Ports 443 und 563, da für ACLs eine UND-Verknüpfung gilt.
- Durch den dritten Eintrag ist alles, was noch nicht verboten ist, für alle erlaubt.

## Weitere Beispiele

1) Nur lokale Nutzung zulassen

Folgendes Beispiel zeigt, wie Sie die Nutzung Ihres Proxys auf Ihre Domain einschränken können. Sie definieren hierfür eine neue Access-Liste mit dem Namen „local" und lehnen alle Zugriffe, die nicht aus der Domain schule.de kommen, ab.

```
acl             local          srcdomain        schule.de
http_access     deny           !local
```

Fügen Sie diese Zeilen an passender Stelle in der Datei `squid.conf` ein. Beachten Sie aber, dass Sie den „http-access"-Eintrag vor der Zeile „http_access allow all" einfügen!

Wenn Sie nun ein SIGHUP (Kommando *kill –1 PID(squid)*) an den Prozess *squid* senden, wird die Konfigurationsdatei neu gelesen und Ihre Änderungen werden aktiv.

2) Keine URLs zulassen, die die Zeichenkette 'sex' enthalten

Folgende Regel verbietet den Zugang auf alle URLs, die die Zeichenkette 'sex' enthalten. Sie können diese Regel natürlich auch für beliebige andere Zeichenketten anwenden.

```
acl             sex            url_regex        sex Sex SEX
http_access     deny           sex
http_access     allow          all
```

Zuerst erfolgt die Definition einer ACL mit dem Namen „sex". In der zweiten Zeile werden, basierend auf dieser ACL, entsprechender Anfragen abgewiesen. Da die Überprüfung auch Groß/Kleinschreibung berücksichtigt, müssen Sie alle Schreibweisen angeben. Weil eine logische ODER-Verknüpfung erfolgt, erhält man dadurch bei allen Schreibweisen die gewünschte Reaktion. In diesem Beispiel wird der Inhalt der gesamten URL auf die Begriffe hin untersucht, so dass auch Zugriffe der Art **FTP://**....sex... verhindert werden.

3) Zugriff auf eine komplette Domäne sperren

Es ist mit einfachen Mitteln möglich, den Zugriff auf eine gesamte Domain zu sperren. Dabei wird der Domain-Name[14] der Zieldomäne in der URL gesucht.

```
acl              blocking         dstdomain        nicht.erlaubt.de
http_access      deny             blocking
http_access      allow            all
```

Im ersten Schritt erfolgt die Definition der ACL "blocking". Als nächstes wird der Zugriff für alle Clients auf die Domain „nicht.erlaubt.de“ verweigert. Mit der letzten Zeile wird wieder alles, was nicht verboten ist, erlaubt.

**Hinweis:** Die Angabe `http_access allow all` in der letzten Zeile darf natürlich nur einmal in der Datei `squid.conf` stehen. Sie wird in den Beispielen lediglich mehrfach genutzt, um die Reihenfolge der Einträge zu verdeutlichen.

4) Parent- und Neighbour-Cache-Konfiguration

Als letztes Beispiel sei gezeigt, was Sie tun müssen, damit nur bestimmte Rechner Ihren Proxy als *parent*- und andere nur als *neighbour*-Cache benutzen können.

Dazu müssen Sie in der Datei /etc/squid.conf nach einer Zeile mit dem Schlüsselwort “miss_access“ suchen. Diese sollte laut Standardeinstellung wie folgt aussehen:

```
miss_access allow all
```

Durch diesen Eintrag ist es jedermann erlaubt, Anfragen an Ihren Porxy zu richten. Wenn die Daten nicht in Ihrem Cache verfügbar sind, wird Ihr Proxy die Daten besorgen und weiterleiten. Um dies zu verhindern, sollten Sie die eben gezeigte Zeile entfernen und durch die folgenden beiden ersetzten.

```
miss_access allow local
miss_access deny !local
```

[14] Wenn dort nur eine IP-Adresse anstelle eines Namens angegeben ist, funktioniert dieses Verfahren nicht wie gewünscht. Nach dem ersten Zugriff in einem solchen Fall wird aber der Name zu der IP-Adresse gesucht, und von da an wird jeder weitere Zugriff auf diese Domain verweigert.

Die ACL *local* wurden bereits in einem vorherigen Beispiel definiert. Die beiden Einträge bewirken, dass Dokumente geliefert werden, die im Cache vorhanden sind. Forderungen zur Übergabe nicht vorhandener Dokumente werden jedoch zurückgewiesen.

## Kontrolle der Logdatei

Wenn Sie Zugangsregeln definiert haben, ist es oft sinnvoll zu beobachten, wann diese Regeln vom Proxy verwendet werden. Wie oben erwähnt, wird jeder Zugriff auf den Proxy in der Datei

`/var/squid/logs/access.log`

mitprotokolliert. Wenn ein Zugriff abgelehnt wurde, enthält der betreffende Eintrag das Wort `TCP_DENIED`. Nachfolgend ein Auszug aus einer acces.log-Datei:

898697101.762 51 10.0.3.62 TCP_HIT/200 1710 GET http://server.alf.es.bw.schule.de/ - NONE/- text/html
**898697107.214 22 10.0.3.62 TCP_DENIED/400 473 GET FTP://server.alf.es.bw.schule.de - NONE/- -**
**898697149.838 27 10.0.3.62 TCP_DENIED/400 459 GET http://www.sex.de/ - NONE/- -**

In den Zeilen 2 und 3 wurde der Zugriff abgelehnt. Die Anfrage stammte von der Station 10.0.3.62. In der ersten Spalte werden Zugriffsdatum und –zeit erfaßt; damit diese im Klartext protokolliert werden, muss ein entsprechender Eintrag in der Datei `/etc/squid.conf` vorgenommen werden (siehe Kap. 0). Zur Erfassung von Benutzernamen anstelle von IP-Adressen muss der *squid*-Quelltext editiert und neu kompiliert werden. Beachten Sie hierfür die Hinweise im Abschnitt `proxy_auth` in der Datei `/etc/squid.conf`.

---



**Übung 8-2:** Definition von Zugangsregeln auf dem Proxy

---

## 8.3.8 Anpassung der Client-Rechner

Damit die Client-Rechner in Ihrem LAN den Proxy verwenden können, müssen Sie ihn im verwendeten Web-Browser eintragen. Beim Netscape Communicator geschieht dies im Menü *Preferences*. Tragen Sie für alle Internet-Dienste die IP-Adresse Ihres Kommunikationsservers sowie die verwendete Portnummer ein (siehe **Abbildung 8-3**).

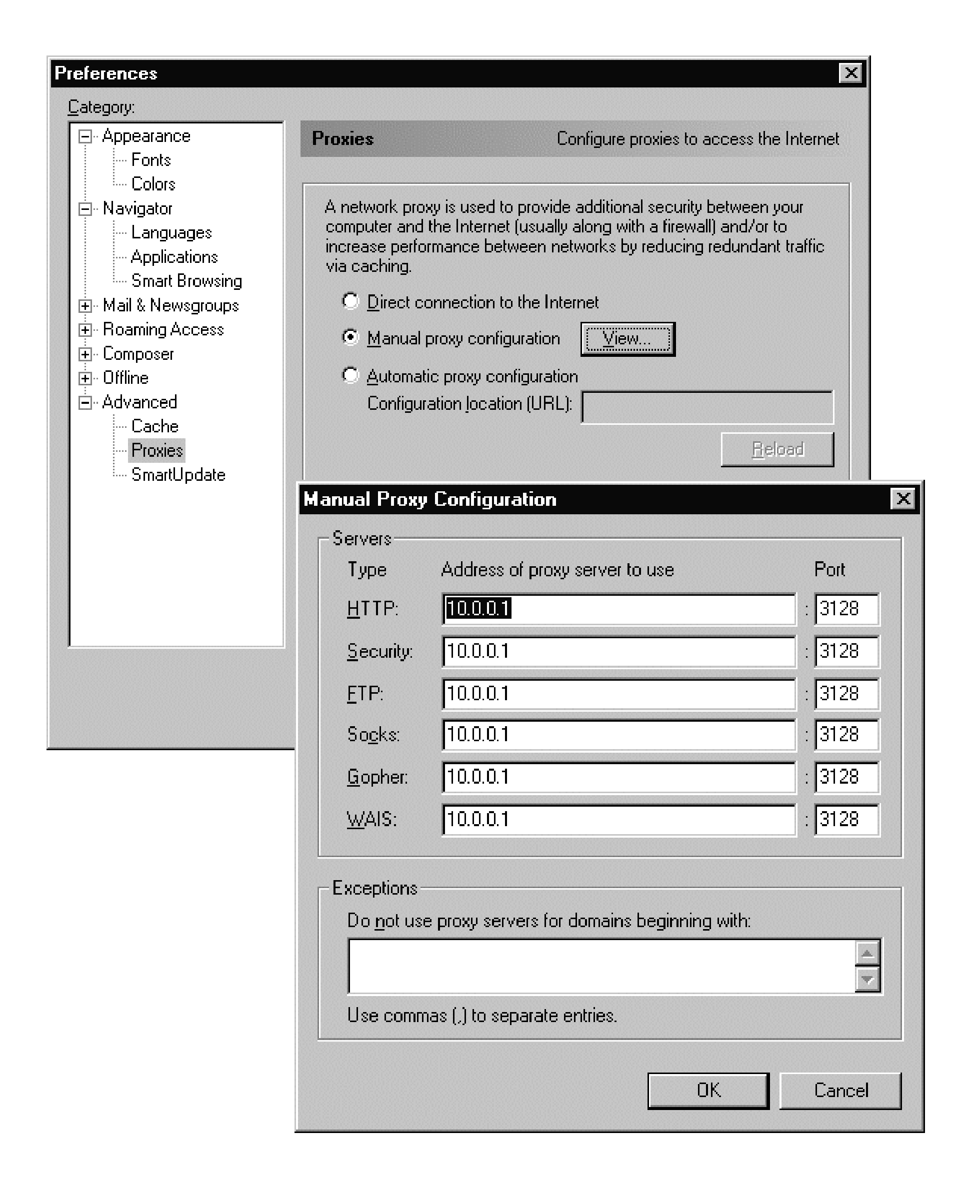



**Abbildung 8-3:** Tragen Sie den Proxy-Server bei den Clients im Netscape-Navigator ein.

# 9 Firewall

Früher wurden zwischen Holzhäusern Mauern aus Stein errichtet, um bei Ausbruch eines Feuers das Übergreifen auf benachbarte Häuser zu verhindern. Diese Feuerschutzmauern heißen im Englischen *firewalls*.

Mit Hilfe eines Firewall-Servers können Sie unberechtigte Zugriffe Ihrer Clients zum Internet und umgekehrt verhindern. Das Funktionsprinzip eines Firewalls ist in **Abbildung 9-1** dargestellt.

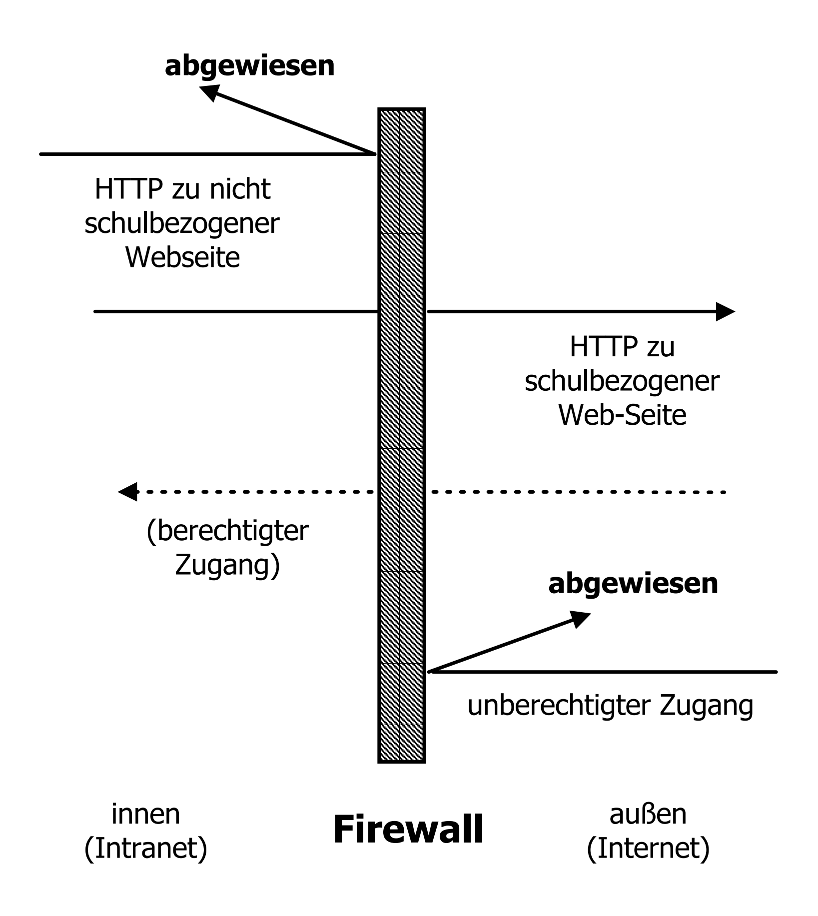



**Abbildung 9-1:** Funktionsprinzip eines Firewalls zwischen dem eigenen LAN (innen) und dem Internet (außen)

Jede Anfrage für einen Datenaustausch zwischen dem Internet und dem eigenen Netz wird vom Firewall auf seine Berechtigung überprüft und gegebenenfalls abgewiesen.

# 9.1 Firewallkonzepte

Man unterscheidet zwischen folgenden drei Firewall-Grundformen:

1) **Paket-Filter** (z.B. IP-Filter)

2) **Circuit-Relays**

3) **Application-Level-Gateways**

Durch die Kombination dieser Grundformen erhält man ein Höchstmaß an Sicherheit.

## Paket-Filter

Paket-Filter analysieren die Datenpakete und können sie nach Sende- und Empfangsadressen, Protokollen (z.B. TCP/IP) oder Portnummern[15] der einzelnen Anwendungen filtern. Dazu werden Zugangsregeln definiert, mit denen nur bestimmte Dienste oder bestimmte Verbindungen erlaubt sind. Die Konfiguration dieser Filterregeln ist aufwendig und bedarf größter Genauigkeit, damit keine Sicherheitslücken entstehen können.

## Circuit-Relays

Circuit-Relays ermöglichen die Nutzung von Applikationen, die auf der Transportprotokollebene (z.B. TCP) aufbauen. Die Verbindungen werden dabei am Eingang des Circuit-Relays unterbrochen und an der Ausgangsseite jeweils neu aufgebaut. Eine direkte Verbindung wird auf dieser Protokollebene verhindert.

## Application-Level-Gateways

Application-Level-Gateways erlauben eine genaue Überwachung von Verbindungen zwischen einem sicheren und einem unsicheren Netz nach vorgegebenen Kriterien. Für die zu nutzenden Applikationen wird dazu ein besonderer Gateway-Dienst (Proxy-Service [s. Kapitel 8]) aufgebaut.

---

[15] Ports kann man sich als Zugangspunkte für Netzwerk-Verbindungen vorstellen. Ein Anwendung bietet im Netz einen Dienst (z.B. FTP) an. Der Dienst verwendet dazu einen bestimmten Port und wartet dort auf zugreifende Clients. Wenn ein Client diesen Dienst nutzen möchte, baut dieser über den Port des Servers eine Verbindung zu dieser Anwendung auf.

# 9.2 Firewall unter Linux

## 9.2.1 Bastionsrechner

Wichtige Daten, die innerhalb eines lokalen Netzes zur Verfügung gestellt werden, müssen natürlich gegen unberechtigten Zugriff (z.B. aus dem Internet) geschützt werden. Der erste Schutzmauer besteht bei Linux in der Verpflichtung, sich am Netzwerk mit Nutzerkennung und Passwort anzumelden.

Als zweiter Schutzmauer kann Ihr Kommunikations-Server als sog. Bastionsrechner dienen, der allen unerlaubten IP-Paketen den Übergang vom Internet in ein Firmennetz verweigert. Die einzelnen Clients aus dem Firmennetz haben in diesem Fall keine direkte Verbindung mit dem Internet, sondern „beauftragen“ den Bastionsrechner die gewünschten Daten aus dem Internet zu holen und bereitzustellen. In diesem Falle sind alle Dienste vom Internet getrennt, die nicht über den Bastionsrechner laufen. Auf dem Bastionsrechner müssen dafür ein Domain Name Server (s. Kapitel 7) und ein Proxy (s. Kapitel 8) arbeiten. Für maximale Sicherheit wird ein Bastionsrechner über einen Router mit dem Internet verbunden. Zusätzlich wird auch das lokale Netz über einen Router mit dem Bastionsrechner angesclossen (Internet – Router – Bastionsrechner – Router – LAN). Diesen Aufwand werden Sie an Ihrer Schule nicht betreiben, so dass Ihr Linux-Server kein "echter" Bastionsrechner ist.

Sie verwenden den Firewall in erster Linie dafür, um jeden Client zur Verwendung des Proxys zu zwingen (siehe Übungsaufgabe). Damit liegt die volle Kontrolle über alle Internet-Zugriffe – insbesondere bei Verwendung von Zugriffsregeln - beim Firewall. Der Schutz vor Angriffen aus dem Internet ist eher zweitrangig, da Sie in Ihrem lokalen Netz nicht-routbare IP-Adressen verwenden und somit die Rechner Ihres LANs vom Internet aus überhaupt nicht sichtbar sind.

## 9.2.2 Einrichtung des Firewalls

Wenn Sie bei der Linux-Installation die Konfiguration *Internet access server* gewählt haben, ist bereits ein Firewall installiert[16], welches nur noch konfiguriert und aktiviert werden muss.

Folgende Konfigurationsdateien sind für die Firewall-Einrichtung von Bedeutung:

- `/etc/rc.config` enthält alle Firewall-Variablen
- `/sbin/init.d/firewall` Skript zum Start des Firewalls
- `/etc/fw-friends` Liste "befreundeter" Rechner

[16] Unter S.u.S.E.-Linux ist das Paket **firewall** in der Serie n (Netzwerk) enthalten.

- /etc/fw-inout — Liste der Rechner mit direktem Zugang zum Internet
- /usr/doc/packages/firewall/README — weitere Informationen zum Firewall

Außerdem finden Sie

- /sbin/init.d/masquerade — Skript zum Start des Masquerading

welches wir bereits verwendet haben. (Kap.: 5.4.3)

Zusätzlich muss der Kernel Firewalling und Masquerading unterstützten. Die S.u.S.E.-Standard-Kernel unterstützen dies seit der Version 5.2.

---

***Achtung:** Bei älteren Distributionen als 5.2 ist es erforderlich, dass Sie den Kernel neu übersetzen und die Optionen Firewalling und Masquerading aktivieren[17].*

---

Im S.u.S.E.-Linux wird der Firewall durch verschiedene Variablen in der allgemeinen Konfigurationsdatei

/etc/rc.config

gesteuert. Diese tragen jeweils das Präfix FW_ und enthalten eine Liste von IP-Adressen oder Rechnernamen. Mehrere Einträge werden durch Leerzeichen voneinander getrennt.

## Übersicht die Variablen des Firewalls

| | |
|---|---|
| FW_START | Dieser Wert muss auf yes geändert werden, damit der Firewall gestartet wird. |
| FW_LOCALNETS | Liste der lokalen Netze. Diese werden geschützt. Auf diese wird Freunden (siehe FW_FRIENDS) der Zugriff gestattet. |
| FW_FTPSERVER | Adressen von FTP-Servern, auf die von außen zugegriffen werden darf. |
| FW_WWWSERVER | Adressen von WWW-Servern, auf die von außen zugegriffen werden darf. |
| FW_SSLSERVER | Adressen von Secure-Socket-WWW-Servern, auf die von außen zugegriffen werden darf. |
| FW_SSSLPORT | Portnummer, auf der die SSL-Server Anfragen erwarten. Hier ist nur eine Nummer möglich. |

[17] Im Kapitel 15 finden Sie dazu eine Anleitung.

| | |
|---|---|
| FW_MAIL-SERVER | Adressen von Mail-(SMTP-)Servern, auf die von außen zugegriffen werden darf. |
| FW_DNSSERVER | Adressen von DNS-Servern, auf die von außen zugegriffen werden darf. |
| FW_NNTPSERVER | Adressen von lokalen NNTP-Servern (vgl. Kap. 14), auf die den NEWS-Feeds von außen der Zugriff erlaubt werden soll. |
| FW_NEWSFEED | Adressen der Newsfeeds, die die NNTP-Server erreichen dürfen. |
| FW_WORLD_DEV | Device, das überwacht werden soll. Hier können auch mehrere Devices angegeben werden. |
| FW_TCP_LOCKED_PORTS | TCP-Portnummern, die gesperrt werden sollen. Hier muss eine Liste von TCP-Port-Bereichen angegeben werden. *Beispiel* 1:6 8:1023 bedeutet, dass die Ports 1 bis 6 und 8 bis 1023 gesperrt sind. |
| FW_INT_DEV | Device zu dem nach innen gerichteten Netz. Über dieses Device werden Verbindungen vom lokalen Netz ins Internet überwacht. |
| FW_LOG_DENY | Steht diese Variable auf 'yes', so werden alle Verletzungen der Firewall-Deny-Regeln in der Datei `/var/log/messages` mitgeschrieben. D.h., dass jeder Versuchfestgehalten wird, den Firewall zu durchdringen. |
| FW_LOG_ACCEPT | Steht diese Variable auf 'yes', so werden alle Pakete, die auf Firewall-Accept-Regeln passen, in die Datei `/var/log/messages` mitgeschrieben. Das heißt, dass jedes Paket, das erlaubterweise durch den Firewall geht, mitprotokolliert wird. |
| FW_ROUTER | Adresse des Internet-Routers. Diese Variable sollte nur dann ausgefüllt werden, wenn der Router eine Adresse aus dem Adreßbereich hat, der in `FW_LOCALNETS` angegeben wurde. |
| FW_INOUT | Steht diese Variable auf 'yes', so wird die Datei `/etc/fw-inout` gelesen. Andernfalls haben alle Rechner aus dem internen Netz vollen Zugriff auf das Internet. |
| FW_TRANS_PROXY_IN | Hier kann eine Liste von Ports und IP-Adressen angegeben werden, um Pakete 'On-the-fly' auf lokale Ports umzuleiten. Es werden hiermit eingehende Verbindungen umgeleitet.. |
| FW_TRANS_PROXY_OUT | Wie `FW_TRANS_PROXY_IN`, jedoch für ausgehende Verbindungen. |
| FW_REDIRECT | Hiermit können lokale Ports zu Ports auf fremden Rechnern umgeleitet werden. Diese Funktion ist noch sehr experimentell und sollte nicht verwendet werden! |
| FW_FRIENDS | Steht diese Variable auf 'yes', so wird die Datei `/etc/fw-friends` gelesen. Andernfalls hat kein Rechner aus dem Internet vollen Zugriff auf das lokale Netz. |
| FW_SSH | Hiermit wird das Freischalten des SSH-Ports (Port 22) für die in `/etc/fw-ssh` aufgelisteten Rechner aktiviert. |
| FW_UDP_LOCKED_PORTS | UDP-Portnummern, die gesperrt werden sollen. Die Synatx ist identisch mit der der TCP-Ports. Sinnvoll für UDP wie TCP ist die Angabe 1:1023, d.h. alle reservierten Ports sind gesperrt. |



## Die Datei `/etc/fw-friends`

In der Datei `/etc/fw-friends` sind alle Rechner eingetragen, die uneingeschränkten Zugriff auf das lokale Netz erhalten sollen. Pro Zeile darf nur ein Rechner eingetragen werden. Kommentarzeilen beginnen mit '#' (Raute). Diese Datei wird nur gelesen, wenn die Variable `FW_FRIENDS` auf 'yes' gesetzt ist.; andernfalls hat kein Rechner aus dem Internet vollen Zugriff auf das lokale Netz.

## Die Datei `/etc/fw-inout`

Nur die Rechner bzw. Netze, die in dieser Datei aufgeführt sind, erhalten direkten Zugriff auf das Internet. Alle anderen Rechner werden vom Firewall geblockt. Kommentarzeilen werden mit # eingeleitet. Diese Datei wird nur gelesen, wenn die Variable `FW_INOUT` auf 'yes' gesetzt ist; andernfalls haben alle Rechner aus dem lokalen Netz vollen Zugriff auf das Internet.

## Start des Firewalls

Zum Starten des Firewalls wird das firewall-Skript

**`/sbin/init.d/firewall`**

aufgerufen, welches unter S.u.S.E.-Linux vier Parameter kennt:

| | |
|---|---|
| `start` | Der Firewall wird gestartet. |
| `stop` | Der Firewall wird gestoppt. |
| `block` | Entspricht dem Ziehen eines Netzwerkkabels, d.h. es geht weder etwas hinein noch heraus. |
| `list` | Die aktuellen Firewall-Regeln werden angezeigt. |

Beispiel zur Aktivierung des Firewalls:

**/sbin/init.d/firewall start [↵]**

## Minimalkonfiguration

An Ihrer Schule reicht es aus, den Firewall mit einer Minimalkonfiguration laufen zu lassen. Folgende Schritte sind hierfür notwendig:

- Editieren der Datei `/etc/rc.config`



Setzen Sie folgende Variablen:

| | |
|---|---|
| `FW_START="yes"` | (startet den Firewall) |
| `FW_LOCALNETS ="134.108.233.128/255.255.255.128 10.0.3.0/255.255.255.0"` | (zu kontrollierende Netze) |
| `FW_WORLD_DEV ="eth0"` | (Device zum Internet) |
| `FW_INT_DEV ="eth1"` | (Device zum LAN) |
| `FW_LOG_ACCEPT ="yes"` | (**nur zu Testzwecken!!!**) |
| `FW_FRIENDS="yes"` | (Zugriff für Freunde vom Internet) |
| `FW_INOUT ="yes"` | (direkter Internetzugriff für best. Rechner aus dem LAN) |
| `FW_TCP_LOCKED_PORTS="1:1023"` | (sperrt alle reservierten Ports[18] ) |
| `FW_DNSSERVER="134.108.233.211/255.255.255.128"` | (Nameserver unserer Domäne) |
| `FW_MAILSERVER="134.108.233.211/255.255.255.128"` | (Mailserver unserer Domäne) |
| `FW_UDP_LOCKED_PORTS="1:1023"` | (w.o., jedoch für UDP-Verbindungen) |

**Achtung:** Die Einträge in der zweiten und dritten Zeile gehören eigentlich in eine Zeile und sind nicht durch ein [↵], sondern durch ein Leerzeichen voneinander getrennt. Der Zeilenumbruch ist in dieser Unterlage nur wegen der geringen Seitenbreite entstanden!

- Aktualisieren Sie Ihre Konfiguration durch Aufruf von:

  **SuSEconfig [↵]**

- Sie können die Konfiguration bei laufendem Firewall abfragen über:

  **ipfwadm –F –l [↵]**

- ***Optional:***

  - Wenn Sie bestimmten Rechnern aus dem Internet direkten Zugriff auf Ihr LAN gestatten wollen, so legen Sie die Datei `/etc/fw-friends` an und tragen die IP-Adressen dieser Rechner dort ein (nur ein Rechner pro Zeile!).

  - Wenn Sie bestimmten Rechnern aus dem LAN direkten Zugriff ins Internet gestatten wollen, so legen Sie die Datei `/etc/fw-inout` an und tragen die IP-Adressen dieser

[18] Sie finden die Portnummern in der Datei `/etc/services`.

Rechner dort ein (nur ein Rechner pro Zeile!).

- Starten Sie den Firewall durch Aufruf von:

  **/sbin/init.d/firewall start [↵]**

- Sie können alle Meldungen Ihres Firewalls (z.B. erlaubte bzw. verbotene Zugriffe beobachten) durch Eingabe von:

  **tail –f /var/log/messages [↵]**

- Wenn Sie sich von der korrekten Funktionsweise überzeugt haben, setzen Sie **unbedingt** in der Datei `/etc/rc.config` die Variable `FW_LOG_ACCEPT` wieder auf '`no`' !!!

  ```
  FW_LOG_ACCEPT="no"
  ```

  Andernfalls sprengt die Datei `/var/log/messages` jeden Rahmen!

- Starten Sie anschließend den Firewall neu über:

  **/sbin/init.d/firewall stop [↵]**
  **/sbin/init.d/firewall start [↵]**

---




---






# 10 File Transfer Protocol (FTP)

Um Dateien auf Ihren Linux-Server zu übertragen, können Sie das FTP-Protokoll verwenden. Sie benötigen dafür auf Ihrer Workstation eine FTP-Client-Software und auf dem Linux-Server einen FTP-Server. Jede Linux-Installation beinhaltet bereits einen voll funktionsfähigen FTP-Server; in SuSE-Linux 5.2 ist der *WU-FTP*-Server, Version 2.4.2, enthalten.

## 10.1 Konfiguration des WU-FTP-Servers

Da Sie an Ihrer Schule nicht notwendigerweise einen FTP-Server benötigen, wird die Konfiguration des FTP-Servers hier nur sehr knapp behandelt. Weitere Informationen und Beispielkonfigurationen finden Sie im Verzeichnis:

`/usr/doc/packages/wuFTPd`

### Konfigurationsdateien

Der FTP-Server wird über folgende Dateien konfiguriert:

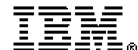
- `/etc/FTPaccess` — Regelt den Zugriff auf den FTP-Server.
- `/etc/FTPconversions` — Legt fest, ob und wie Dateien beim Up- oder Download komprimiert bzw. entpackt werden.
- `/etc/FTPusers` — Benutzer, die FTP ***nicht*** verwenden dürfen.

Wie oben erwähnt, ist der FTP-Server *ohne* Veränderung dieser Konfigurationsdateien einsatzbereit. Wenn Sie es jedoch wünschen, editieren Sie nach Bedarf diese Dateien und starten den FTP-Server neu.

## 10.2 Einrichtung des FTP-Clients WS_FTP

Um von Ihrer Workstation auf einen FTP-Server zugreifen zu können, benötigen Sie eine FTP-Clientsoftware. Es bieten sich hierfür zwei Möglichkeiten an:

- Sie können entweder eine MS-DOS-Eingabeaufforderung starten und das Kommando **FTP *FTP-Server*** (z.B.: FTP 10.0.0.1) eingeben. Dann müssen Sie jedoch die FTP-Kommandos kennen und von Hand eingeben.



- Alternativ verwenden Sie eine Client-Software mit grafischer Benutzeroberfläche. Hier bietet sich das Freeware-Programm` **WS_FTP`** an[19].

Beim der Verwendung des FTP-Protokolls wird unterschieden, ob binäre Dateien (ausführbare o.ä.) bzw. ASCII-Dateien übertragen werden. Es kann daher geschehen, dass Dateien nach der Übertragung unbrauchbar sind, da FTP im ASCII-Modus einen anderen Übersetzungsalgorithmus verwendet als im binären Modus. Der `WS_FTP`- Client von Ipswitch verfügt über einen "Auto"- Modus, der die zu übertragenden Dateien überprüft und selbst den korrekten Modus wählt. Hierdurch können Fehler vermieden werden.

---

**Übung 10-1:** Installation und Verwendung eines FTP-Clients

---

[19] kostenloser Download z.B. über FTP://FTP.uni-marburg.de/pub/dos/komm/winsock/ws_FTP32.zip

# 11 "Apache" Web-Server

Auf Ihrem Linux-Server läuft bereits der vollwertige Web-Server: *Apache.* Sie werden ihn jedoch nicht verwenden, um Informationen für Clients aus dem Internet bereitzustellen. Grund hierfür ist, dass Sie über eine ISDN-Wählleitung mit dem Internet verbunden sind und die Leitung nur für Anfragen von der Schule ins Internet geöffnet wird.

Sie können jedoch Ihren Web-Server als Intranet-Server verwenden, d.h. über das HTTP-Protokoll den Clients in Ihrem LAN (Ihrer Schule) Informationen bereitstellen. Wenn Sie Informationen über Ihre Schule im Internet veröffentlichen wollen, bietet Ihnen BelWü einen sog. "virtuellen Web-Server" auf einem ihrer Server an. Dieser virtuelle Web-Server kann im Internet über den Namen Ihrer Domäne angesprochen werden, also z.B. http://www.schule1.alf.es.bw.schule.de . Sie müssen lediglich Ihre Webseiten auf diesen Server via FTP übertragen (siehe Kapitel 10). Die Verwaltung und Wartung dieses öffentlich zugänglichen "schuleigenen" Web-Servers übernimmt dann das BelWü.

## Ziele dieses Kapitels

Konfigurieren des Apache Web-Servers

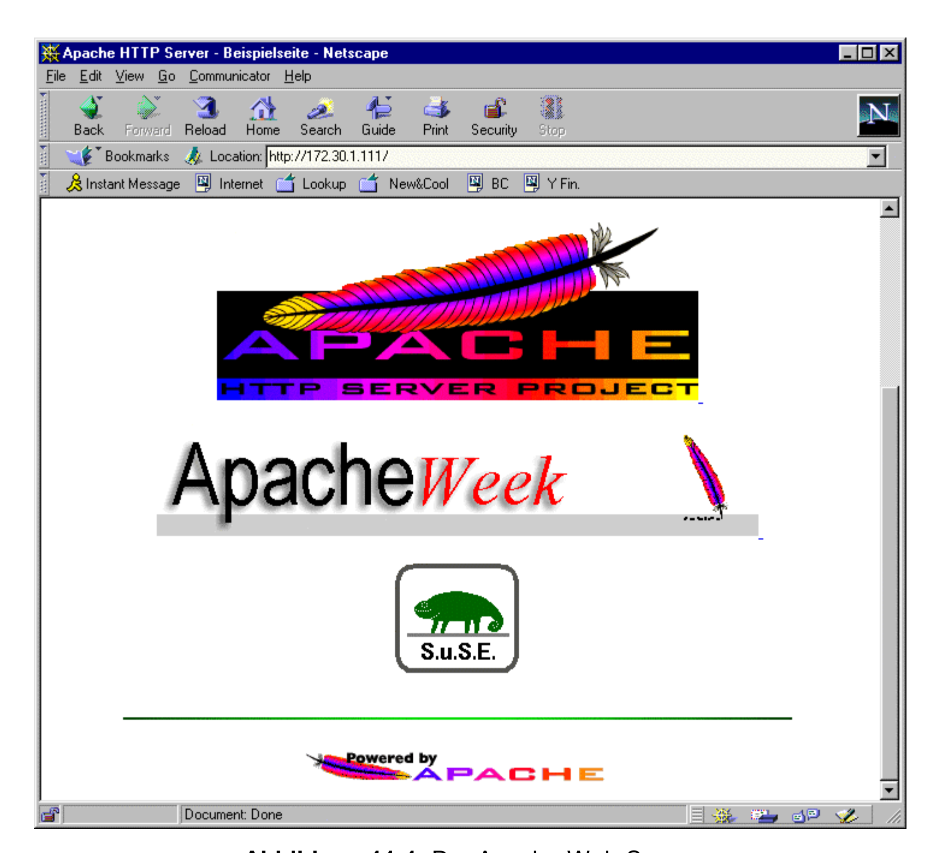



**Abbildung 11-1:** Der Apache-Web-Server

# 11.1 Konfiguration des "Apache"

Unter SuSE-Linux 5.2 ist die Version 1.2.0 des Web-Servers *apache* bereits installiert, wenn Sie bei der Linux-Installation die Konfiguration *Internet access server* gewählt haben[20].

## 11.1.1 Verzeichnisse

Mit der *apache*-Installation wird ein neues Unterverzeichnis

`/usr/local/httpd`

angelegt. Dieses enthält wiederum die Unterverzeichnisse[21]

- `/htdocs` Zum Ablegen der HTML-Dokumente auf dem Web-Server.
- `/cgi-bin` Nimmt Programme auf, die vom Web-Server gestartet werden sollen.
- `/icons` Enthält Icons, die vom Web-Server erreichbar sein müssen.

Mit der *apache*-Installation werden im Verzeichnis `/usr/local/httpd/htdocs` eine Reihe von HTML-Dokumenten abgelegt, die unter anderem die **Apache-Dokumentation** und das **SuSE-Hilfesystem** beinhalten. Starten Sie einfach auf einem beliebigen Client einen Web-Browser und geben Sie als Ziel Ihren Linux-Server an.

## 11.1.2 Konfigurationsdateien

Die Konfigurationsdateien befinden sich im Verzeichnis

`/etc/httpd`.

Sie finden hier die Dateien

- `httpd.conf` Konfiguration des Web-Servers.
- `access.conf` Zugangsregelung zum Web-Server.
- `srm.conf` Konfiguration der Web-Server-Ressourcen.

[20] Alternativ installieren Sie mit Hilfe von `Yast` das Paket **apache** aus der Serie **n**.

[21] Bei älteren SuSE-Distributionen finden sich alle für den Web-Server relevanten Dateien unterhalb von `/httpd`. Die Konfigurationsdateien sind dann meistens unter `/httpd/conf` abgelegt. Ferner ist auch `/usr/local/etc/httpd/conf` ein oft verwendeter Platz.

- `mime.types` Auflistung der MIME-Typen.

In älteren apache-Versionen war man gezwungen, die einzelnen Konfigurationsanweisungen in die jeweils richtige der ersten drei Dateien zu verteilen. Inzwischen ist es prinzipiell möglich, fast alle Konfigurationsanweisungen beliebig auf die drei Dateien zu verteilen. Da eine Aufteilung auf einzelne Dateien jedoch die Übersichtlichkeit erhöht, sollte man diesem Vorgehen den Vorzug geben.

Weiterhin können jeweils Konfigurationen für einen Zugriffsschutz in lokalen *.htaccess*-Dateien definiert werden. Beim Zugriff des *Apache* auf ein Verzeichnis überprüft dieser als erstes, ob sich dort oder weiter unten im Dateibaum derartige Dateien auffinden lassen. Ist dies der Fall, so werden sie entsprechend der Angaben in den globalen Konfigurationsdateien ausgewertet.

### 11.1.3 Start des Web-Servers

Der Apache-Web-Server kann manuell gestartet werden durch Aufruf des Shell-Skripts

**/sbin/init.d/apache start [↵]**

Der automatische Start wird durch den (bereits vorhandenen) Eintrag

```
START_HTTPD=yes
```

in der allgemeinen Konfigurationsdatei `/etc/rc.config` erreicht.

### 11.1.4 Minimalkonfiguration

Sie müssen am Apache-Web-Server ausgesprochen wenig konfigurieren. Lediglich folgende Punkte sind sinnvoll:

#### Editieren der Datei `/etc/httpd/httpd.conf`

Die Datei `httpd.conf` ist die einzige für Sie wichtige Konfigurationsdatei. Sehen Sie sich die Datei mit einem Editor an und probieren Sie ruhig einige Optionen aus; alle Optionen sind mit Kommentaren versehen.




- Logdatei

Jeder Zugriff auf Ihren Web-Server wird in der Datei

```
/var/log/httpd.access_log
```

mitprotokolliert. Sie können entscheiden, ob hier der Name der abfragenden Clients eingetragen wird (default), oder nur deren IP-Adresse. Namensauflösungen erfordern zusätzliche Abfragen, so dass sich möglicherweise die Performance Ihres Web-Servers verringert (siehe Kommentar). Insbesondere bei Anfragen von Clients, die nicht im DNS eingetragen sind, kann sich der Zugriff dramatisch verlangsamen, da der Name nicht aufgelöst werden kann. Dann muss man bis zu einem *timeout* gewarten (ca. 1 min). Der zugehörige Abschnitt für abgeschalteten DNS-Lookup lautet:

```
# HostnameLookups: Log the names of clients or just their IP numbers
#   e.g.   www.apache.org (on) or 204.62.129.132 (off)
# You should probably turn this off unless you are going to actually
# use the information in your logs, or with a CGI.  Leaving this on
# can slow down access to your site.
HostnameLookups off
```

- Administrator des Web-Servers

Tragen Sie ein, wem per E-Mail Probleme mit dem Web-Server mitgeteilt werden sollen. Der zugehörige Eintrag lautet:

```
# ServerAdmin: Your address, where problems with the server should
# be e-mailed.

ServerAdmin webmaster@schule1.alf.es.bw.schule.de
```

- Name des Web-Servers

Ferner ist es sinnvoll, dass der Web-Server "seinen eigenen Namen kennt". Sie finden hierzu den Abschnitt:

```
# ServerName allows you to set a host name which is sent back to
# clients for your server if it's different than the one the program
# would get (i.e. use "www" instead of the host's real name).
#
# Note: You cannot just invent host names and hope they work. The
# name you define here must be a valid DNS name for your host. If
```



```
# you don't understand this, ask your network administrator.

ServerName server.schule1.alf.es.bw.schule.de
```

**Achtung:** Wie bereits im Kommentar vermerkt, muss hier der "echte" DNS-Name stehen (der Name, unter dem Ihr Server im Internet bekannt ist)!

### Anlegen eines Unterverzeichnisses für Homepages

Damit Ihre Schüler Homepages auf dem Web-Server ablegen können, legen Sie am besten ein zentrales Unterverzeichnis unter `/usr/local/httpd` an. Nennen Sie es beispielsweise `smv` (Schüler-Mitverantwortung). Dies geschieht mit dem Kommando

**mkdir /usr/local/httpd/htdocs/smv [↵]**

Damit jeder dort html-Dokumente ablegen kann, müssten Sie noch die Zugriffsrechte ändern:

**chmod ugo+rwx /usr/local/httpd/htdocs/smv [↵]**

Dies geschieht jedoch schon automatisch!!

Ihre Schüler können nun via FTP im Verzeichnis `smv` beliebige Webseiten ablegen.

### Anlegen von Unterverzeichnissen für individuelle Homepages

Wenn Ihre Schüler über Benutzerkennungen und Home-Directories auf dem Linux-Server verfügen, können sie auf einfache Weise persönliche Homepages ablegen. Folgende Schritte sind hierfür notwendig:

- Anlegen eines Verzeichnisses `public_html` im jeweiligen Stammverzeichnis, z.B. für den Benutzer "weber":

  **mkdir /home/weber/public_html [↵]**

- Ändern der Zugriffsrechte für dieses Verzeichnis:

  **chmod ugo+rx /home/weber/public_html [↵]**

- Kopieren (mit FTP, telnet oder Samba) der betreffenden Webseiten in dieses Verzeichnis und ggf. Zugriffsrechte ändern: **chmod ugo+rx /home/weber/public_html/* [↵]**

- Die Webseiten sind dann abrufbar unter

  `http://Web-Servername/~Benutzerkennung/Name_der_Webseite`

  Wenn der Benutzer *weber* eine Seite namens `index.html` als Startseite abgelegt hat, kann diese z.B. abgerufen werden unter:

  `http://10.0.0.1/~weber`

  In diesem Fall muss nicht der Name der Webseite angegeben werden, da entprechend üblicher Konventionen automatisch die Seite mit dem Namen `index.html` geladen wird.

### Überspielen der Webseiten zum virtuellen Web-Server bei BelWü

Wenn Sie die Schülerwebseiten im Internet anbieten wollen, so müssen Sie sie auf den virtuellen Web-Server des Providers BelWü überspielen. Sie können hierfür entweder eine Workstation mit einem FTP-Client verwenden (z.B. \`WS_FTP\`, siehe Kap. 10.2), oder direkt von Ihrem Linux-Server eine FTP-Verbindung aufbauen. Hierfür bietet sich z.B. unter Xwindows das Programm *xFTP* an, das ähnlich funktioniert wie \`WS_FTP\` und daher nicht weiter besprochen wird.

---

 **Übung 11-1:** Konfiguration des Apache-Web-Servers

---

# 12 Samba

Linux bietet Ihnen die Möglichkeit, Verzeichnisse auf dem Linux-Server an ein Microsoft-Netz freizugeben. Diese Verzeichnisse sehen dann genauso aus, als wären Sie von einem Windows-Rechner freigegeben worden. Die hierfür benötigte Software heißt *Samba* und wird Ihnen mit Linux mitgeliefert.

Sie können Samba insbesondere dafür nutzen, das Verzeichnis `/usr/local/httpd/htdocs`, in dem sich Ihre Webseiten befinden, an das Microsoft-Netz freizugeben. Somit benötigen Sie zur Übertragung neuer Webseiten zum Linux-Server keine FTP-Software mehr, sondern können einfach den Windows-Explorer verwenden.

## 12.1 Grundlagen

NetBIOS ist ein von Microsoft entwickeltes Netzwerkprotokoll, mit dem Rechner mit microsoftbasierten Betriebssystemen (Windows for Workgroups, Windows 95, Windows NT, MS-DOS) untereinander kommunizieren können.

Das SMB-Protokoll (Server Message Block) baut auf NetBIOS auf; mit SMB können verschiedenen Rechner Festplattenverzeichnisse und Drucker miteinander teilen. Jeder Rechner kann Verzeichnisse freigeben. Die anderen Rechner können sich dann unter Angabe des Rechnernamens und des Freigabenamens mit diesem Verzeichnis verbinden. Auch Drucker können unter Angabe eines Rechner- und Freigabenamens mitbenutzt werden.

Da NetBIOS nur ein Netzwerkprotokoll (kein Transportprotokoll) ist, setzt es auf der Transportschicht auf und kann über ein beliebiges Transportprotokoll übertragen werden (NetBEUI, IPX/SPX[22] oder TCP/IP). Besonders interessant ist, dass NetBIOS-Daten in TCP/IP-Pakete verpackt werden können: Internet- und Intranet-Zugriffe können über dasselbe Netzwerktransportprotokoll abgewickelt werden. Dies verringert die Installations- und Wartungskosten, da an den Clients nur ein Protokoll konfiguriert und geroutet werden muss. Zum anderen lässt sich über das Internet auch problemlos auf Verzeichnisse von Rechnern zugreifen, die in räumlich entfernten Filialen des Unternehmens stehen.

Inzwischen gibt es das SMB/NetBIOS-Protokoll auch für nicht-Microsoft-Rechner, wie z.B. Unix. Das Programm heißt *Samba* und befindet sich auf der SuSE-CD in der Paketserie ***n*** im Paket ***samba***. Den Quellcode können Sie im Internet finden. Samba hat die Homepage:

```
http://samba.canberra.edu.au/pub/samba
```

[22] NetBEUI ist ein von Microsoft entwickeltes, relativ einfaches Transportprotokoll, das speziell für NetBIOS entwickelt wurde. IPX/SPX ist ein Protokoll, das in Novell-Netzwerken verwendet wird.

# 12.2 Netzlaufwerke freigeben

Samba wird bei der gewählten Konfiguration *Internet access server* automatisch mitinstalliert. Die Konfiguration erfolgt über die Datei

`/etc/smb.conf`

Um Verzeichnisse freizugeben, müssen diese und evtl. gewünschte Optionen in die Datei `/etc/smb.conf` eingetragen werden.

## Konfigurationsschritte

Nachfolgend wird Ihnen beschrieben, wie Sie das Verzeichnis

`/usr/local/httpd/htdocs/smv`

welches die Webseiten Ihrer Schüler enthalten soll, ans Microsoft-Netz freigeben.

- Verzeichnis anlegen und Zugriffsrechte erteilen

Das freizugebende Verzeichnis `/usr/local/httpd/htdocs/smv` muss natürlich existieren und sollte unter Linux für jeden les- und schreibbar sein. Falls es noch nicht existiert, legen Sie es an und vergeben die gewünschten Zugriffsrechte:

**mkdir /usr/local/httpd/htdocs/smv [↵]**
**chmod ugo+rwx /usr/local/httpd/htdocs/smv [↵]**

- Editieren der Datei `/etc/smb.conf`

Wenn Sie mehrere Netzwerkkarten verwenden und ein Firewall aktiv ist (dieser blockiert Samba-Freigaben!), so geben Sie zunächst die Netzwerkkarte an, die mit Ihrem LAN verbunden ist, auf der die Freigabe erfolgt. Sie finden hierzu die Zeile `interfaces`:

```
interfaces = 10.0.0.1/255.255.255.0
```

Für jedes freizugebende Verzeichnis legen Sie in der Datei `/etc/smb.conf` einen eigenen Abschnitt an. Dieser beginnt mit dem Freigabenamen in eckigen Klammern, welcher nicht länger als 8 Buchstaben sein sollte. Für unser Beispiel wäre das:




```
[smv]
comment = Schueler-Webseiten
path = /usr/local/httpd/htdocs/smv
public = yes
browseable = yes
read only = no
```

Sie können im Parameter `comment` für jede freigegebene Ressource einen Kommentar angeben, der dann z.B. beim Verbinden im Windows-Explorer angezeigt wird. Der lokale Laufwerkspfad zu der Ressource wird durch den Parameter `path` bestimmt. Mit `public` wird festgelegt, ob Benutzer ohne Namen/Passwort-Anfrage auf die Ressource zugreifen dürfen (mögliche Werte: `yes` oder `no`); Wenn die Freigabe sichtbar sein soll, verwenden Sie den Parameter `browseable` und setzen ihn auf 'yes'. `read only` legt fest, ob die Ressource schreibbar (`no`) oder schreibgeschützt (`yes`) exportiert werden soll.

Mehrere freigegebene Verzeichnisse werden in der Konfigurationsdatei hintereinander aufgeführt:

```
[smv]
comment = Schueler-Webseiten
path = /usr/local/httpd/htdocs/smv
public = yes
browseable = yes
read only = no

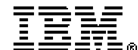
[cdrom]
comment = Linux CD-ROM
path = /cdrom
public = yes
read only = yes
```

- Start von Samba

Samba wird durch Aufruf zweier Dämonen gestartet („Die Geister, die ich rief...“.).

**nmbd –D [↵]**
**smbd –D [↵]**

Hierbei sorgt der Samba-Dämon `smbd` für die eigentliche Freigabe, während mit dem NetBIOS-Dämonen `nmbd` der Namensdienst für NetBIOS organisiert wird. Der Parameter `D` steht für die Dämon-Betriebsart.



- Verbinden mit der freigegebenen Ressource

Will sich ein Microsoft Windows-Rechner mit der freigegebenen Ressource verbinden, so ist folgendes zu beachten:

- Der NetBIOS-Name des freigebenden Linux-Servers ist der DNS-Rechnername ohne Domain-Angabe (also z.B. **`server`** bei `server.schule1.alf.es.bw.schule.de`). NetBIOS-Rechnernamen dürfen maximal 15 Buchstaben lang sein, daher kann es bei langen DNS-Namen zu Komplikationen kommen[23].

- Der komplette Laufwerkpfad, der Windows im Verbinden-Dialog eingegeben werden muss, lautet in unserem Beispiel:

```
\\server\smv
```

- Eine schöne Methode, freigegebene Ressourcen anzeigen zu lassen, ist folgende: Gehen Sie auf Ihrer Windows 95/NT-Workstation auf **Start → Ausführen ...** und geben Sie einfach den Rechnernamen ein, z.B.:

**\\server [↵]**

Sie brauchen dann nicht zu wissen, welche Ressourcen freigegeben sind bzw. welcher Arbeitsgruppe der Rechner angehört.

- Samba-Aktualisierung

Nach jeder Änderung an der Konfigurationsdatei `/etc/smb.conf` muss Samba beendet und neu gestartet werden. Das Beenden von Samba geschieht mit dem *killall*-Befehl:

**killall smbd [↵]**
**killall nmbd [↵]**

- Automatischer Samba-Start

Wenn Samba beim Booten automatisch gestartet werden soll, setzen Sie in der allgemeinen Konfigurationsdatei `/ect/rc.config` die Variable `START_SMB` auf 'yes':

```
START_SMB="yes"
```

[23] Ein anderer NetBIOS-Name kann beim Start des NetBIOS-Dämonen durch Angabe des Parameters **`-n`** festgelegt werden: `nmbd -D-n server`

Sie können in diesem Fall Samba durch Eingabe von

**/sbin/init.d/smb stop [↵]**

beenden und mit

**/sbin/init.d/smb start [↵]**

neu starten.

## 12.3 * Weitergehende Konfiguration (optional)

Samba leistet wesentlich mehr, als die einfache Freigabe von Verzeichnissen. Nachfolgend weitere Hinweise zur Konfiguration, die jedoch in diesem Kurs nicht von Belang sind.

- Globale Parameter

Wenn bestimmte Parameter für alle Ressourcen gelten sollen, werden sie am Anfang der Konfigurationsdatei `/etc/smb.conf` unter dem speziellen Service-Namen `global` angegeben:

```
[global]
workgroup = arbeitsgruppe
server string = Samba %v
strict locking = yes
```

Mit dem Parameter `workgroup` legen Sie fest, welcher Windows-Arbeitsgruppe der Samba-Server zugeordnet wird.

Der `server string` legt die Server-Beschreibung fest, wie sie z.B. in der Browse-Liste von Windows 3.11 angezeigt wird; `%v` ist ein Makro (erkennbar am „%"-Zeichen) und wird durch die aktuelle Versionsnummer von Samba ersetzt. Der Server-String darf keine Anführungszeichen enthalten, sonst erscheint unter gewissen Umständen der gesamte Server nicht in der Browse-Liste.

`strict locking` schützt die Dateien vor gleichzeitigem Zugriff von mehreren Nutzern, ähnlich wie das DOS-Programm `share.exe` bei Windows 3.11.






- Private Verzeichnisse

Wenn es auf dem Linux-Server mehrere Benutzer gibt, die ein eigenes Stammverzeichnis besitzen (Home-Directory), so braucht nicht jedes Verzeichnis einzeln in der `smb.conf`-Datei aufgeführt sein. Die Freigabe aller Home-Verzeichnisse für den jeweiligen User wird in der `homes`-Sektion definiert. Diese ist bereits vorhanden und muss nicht editiert werden:

```
[homes]
comment = Heimatverzeichnis
browseable = no
read only = no
create mode = 0700
```

Damit kann sich jeder Benutzer, der ein Account auf der Linux-Maschine hat, via SMB mit seinem Home-Verzeichnis verbinden. Gibt es z.B. einen User „weber“, so kann er von einem Windows-Rechner aus mit:

```
\\server\weber
```

und seinem Unix-Passwort sein Home-Verzeichnis erreichen.

Die Einstellung `browseable = no` verhindert, dass die Freigabe `homes` in der Netzwerkumgebung sichtbar wird. Jeder Benutzer kann sein Heimatverzeichnis nur unter seinem Benutzernamen erreichen.

Da Windows-Rechner keine Unix-Zugriffsrechte kennen, werden mit dem Parameter `create mode` die Zugriffsrechte für neu angelegte Dateien festgelegt.

- Netzdrucker freigeben

Die Freigabe eines Netzwerkdruckers setzt voraus, dass Sie über `Yast` einen Drucker installiert haben (Eintrag in der Datei `/etc/printcap`). Samba gibt per default alle installierten Drucker ans Netz frei.



# 13 E-Mail

In diesem Kapitel lernen Sie, mit Hilfe des Linux-Mailtransportsystems *sendmail* und des E-Mail-Clients *Netscape Messenger* ein E-Mailsystem zu installieren und konfigurieren. Damit sind Ihre Benutzer in der Lage, sowohl in Ihrem LAN, als auch weltweit elektronische Post auszutauschen.

**Ziele dieses Kapitels:**

1. Beschreiben der Bestandteile eines E-Mailsystems.
2. Installieren und konfigurieren des Linux Mail-Servers.
3. Konfigurieren des Netscape Messenger Mail-Clients.

## 13.1 Überblick

Ein E-Mailsystem besteht aus einem *Mail-Server* und in der Regel aus mehreren *Mail-Clients*. Diese Komponenten erfüllen folgende Aufgaben:

**Mail-Server**

- verwaltet den Empfang und die Zustellung von E-Mails
- nimmt E-Mails von einem sog. *Mail Relay Host*[24] entgegen, die vom Internet an Empfänger im lokalen Netz gesendet wurden und umgekehrt

**Mail-Client**

- läuft individuell auf jedem Client-Rechner im LAN
- wird zum Lesen, Schreiben und Beantworten von E-Mail verwendet
- benachrichtigt den Empfänger über neu eingegangene E-Mail

[24] ein Server außerhalb Ihres LANs, der Ihnen E-Mail für Ihre Internet-Domäne zustellt (hier: ein BelWü-Server)

## Prinzipielle Funktionsweise

Auf Ihrem Linux-Server ist bereits das E-Mail-Transportsystem *sendmail* installiert. Sendmail ist für den Empfang und das Versenden von E-Mail ins Internet über das *Simple Mail Transport Protocol* SMTP zuständig. Damit diese E-Mail den adressierten Benutzer erreicht, werden auf dem Mail-Server sog. *Mailboxen* verwendet, in die die Mail einsortiert wird. Will ein Benutzer von seinem PC aus die Mail aus seiner Mailbox abholen, benötigt er einen E-Mail-Client. Dieser baut eine einfache TCP/IP-Verbindung mit dem Mail-Server auf und holt die eingegangene Mail aus der Mailbox ab. Dies geschieht mit Hilfe des *Post Office Protocols* POP. Der Zugang zum Postfach auf dem Mail-Server funktioniert prinzipiell genau wie bei einem Login-Vorgang. Dafür werden eine Benutzerkennung und ein Passwort benötigt. Die Benutzerkennung wird bei der Konfiguration des Mailclients eingetragen. Das Passwort wird bei Bedarf abgefragt.

Auch für das Schreiben und Versenden wird zunächst der E-Mail-Client auf dem lokalen PC verwendet, welcher die zu versendende Nachricht dem Mail-Server zustellt. Dieser stellt fest, ob die E-Mail für einen Empfänger im lokalen Netz bestimmt ist und sortiert sie ggf. in die Mailbox des Empfängers ein.

Befindet sich der Empfänger der E-Mail außerhalb des lokalen Netzes, kann der lokale Mail-Server entweder selbst den entfernten Mail-Server im Zielnetz kontaktieren, oder er bedient sich eines sog. *Mail-Relay*-Servers. Ein Mail-Relay-Server nimmt sämtliche E-Mails für und von unserem lokalen Mail-Server entgegen und sorgt dann selbst für die korrekte Zustellung. Dies ist besonders dann hilfreich, wenn man nur über eine Wählleitung mit dem Internet verbunden ist.

Sie werden im folgenden lernen, Ihren Mail-Server für die Verwendung des Mail-Relay-Servers beim Provider BelWü zu konfigurieren.

# 13.2 Pop-Protokoll

Wie oben erwähnt, wird für die Zustellung von E-Mail in Mailboxen meistens das Pop-Protokoll (POP3) verwendet[25]. Hierfür finden Sie in SuSE-Distributionen in der Paketserie ***n*** das Paket ***pop***, welches bei Ihnen bereits installiert ist. Dieses Paket enthält unter anderem das Programm *popper*. Dies ist der DämonProzess, der die Anforderungen der Mail-Clients entgegennimmt und beantwortet. Es ist somit Grundvoraussetzung, dass dieses Programm auf dem Server aktiviert ist. Dieser Prozess wird üblicherweise vom Internet-Dämon *inetd* aufgerufen. Damit dies möglich ist, muss in dessen Konfigurationsdatei **/etc/inetd.conf** ein Eintrag folgender Form vorhanden sein:

```
pop3 stream tcp nowait root   /usr/sbin/popper -s
```

[25] Eine verbreitete Alternative ist das *Interactive Mail Access Protocol* IMAP.

Falls dieser Eintrag fehlt oder auskommentiert ist, so muss er nachgetragen oder aktiviert werden. Dabei ist zu beachten, dass nach jeder Änderung an dieser Datei dem Prozess *inetd* ein SIGHUP (*kill –1 PID(inetd)*) gesendet werden muss.

## E-Mail-Accounts

Für die Zustellung von E-Mail wird ein E-Mail-Account benötigt (E-Mail-Benutzerkonto). Jeder Benutzer, den Sie auf Ihrem Linux-Server einrichten, erhält automatisch auch ein E-Mail-Account. Seine Mail wird in der Datei:

`/var/spool/mail/Login-Name`

abgelegt.

## 'Nur-E-Mail'-Benutzer

Benutzer, die nur E-Mail verwenden, benötigen weder ein Stammverzeichnis (Home-Directory) noch irgendwelchen weiteren Zugang zum Linux-Server. Verfahren Sie für diese Benutzer wie folgt:

- Legen Sie mit `Yast` eine neue Benutzergruppe, z.B. *E-Mailusers* an, in die Sie später alle 'Nur-E-Mail'-Benutzer aufnehmen können. Diese werden dann *nicht* Mitglied der Standardgruppe *users*.

- Legen Sie mit `Yast` für diese Benutzer entsprechende Benutzerkennungen an, tragen Sie sie in die Gruppe *E-Mailusers* ein und geben Sie als Stammverzeichnis `/tmp` an.

- Tragen Sie mit `Yast` für diese Benutzer als Login-Shell das Passwort-Kommando (`/bin/passwd`) ein. Hierdurch wird erreicht, dass der Benutzer nach einem Login nur sein Passwort ändern kann und danach sofort wieder abgemeldet wird; er erhält also keinerlei weiteren Zugang zum System.

## 13.3 Minimalkonfiguration des Mail-Servers

Wie oben erwähnt, ist das Paket ***sendmail*** aus der Serie ***n*** bei jeder SuSE-Linux-Installation bereits installiert und muss nur noch konfiguriert werden.

Wichtig für das einwandfreie Arbeiten von *sendmail* ist eine korrekte DNS-Konfiguration. Da E-Mail-Adressen grundsätzlich Rechner*namen* und keine IP-Adressen beinhalten, kann keine E-Mail zugestellt werden, wenn die Namensauflösung in Ihrem System nicht funktioniert

Die eigentliche Konfigurationsdatei für *sendmail* ist

`/etc/sendmail.cf`

Da diese jedoch recht schwierig zu handhaben ist, können Sie alle wichtigen Einstellungen durch Editieren der allgemeinen Konfigurationsdatei

`/etc/rc.config`

vornehmen und anschließend `SuSEconfig` aufrufen. Hierdurch wird automatisch eine neue `/etc/sendmail.cf` generiert, die Ihre Einstellungen enthält.

Folgende Einträge müssen in der Datei `/etc/rc.config` für ein funktionierendes Mailsystem vorhanden sein:

(**Achtung:** Die beiden ersten Einträge finden Sie im allgemeinen Teil der Datei `rc.config`, während sich alle weiteren im "Anhang" hinter den ISDN-Einstellungen befinden)

- SMTP aktivieren

Um E-Mails aus dem Internet empfangen zu können, muss der Mailer-Dämon am SMTP-Port aktiv sein. Dies ist die Standardeinstellung. Der zugehörige Eintrag lautet:

```
SMTP="yes"
```

- Absender-Zeile

Beim Versand von E-Mails wird dieser Domänen-Name angegeben. Falls er fehlt, wird der Standard-Domänen-Name (FQDN) des Mail-Servers verwendet, in dem noch der Rechner-

name (z.B. ***server***.schule1.alf.es.bw.schule.de) enthalten ist. Der zugehörige Eintrag könnte wie folgt lauten:

```
FROM_HEADER="schule1.alf.es.bw.schule.de"
```

- Automatisches Anlegen der Datei `/etc/sendmail.cf`

Damit `SuSEconfig` jede Änderung der Mailparameter in die sendmail-Konfigurationsdatei `/etc/sendmail.cf` überträgt, muss der zugehörige Parameter auf "yes" stehen. Dies ist die Standardeinstellung.

```
SENDMAIL_TYPE="yes"
```

- Mail-Relay-Server des Providers (BelWü)

Alle nicht lokalen Mails sollen dem Mail-Server des Providers (BelWü) übergeben werden. In der Datei `rc.config` wird dieser Mail-Server `SMARTHOST` genannt. Tragen Sie hier die IP-Adresse (oder den Namen) des Mail-Servers Ihres Providers ein; bei BelWü ist das 129.143.2.4 (*noc2.BelWue.DE):*

```
SENDMAIL_SMARTHOST="129.143.2.4"
```

- Lokale E-Mail

Sendmail muss wissen, welche E-Mail als lokal angesehen und lokal abgespeichert wird. Tragen Sie hier – jeweils durch ein Leerzeichen getrennt - den Namen Ihres Mail-Servers und evtl. vorhandene Aliasnamen ein:

```
SENDMAIL_LOCALHOST="localhost server.schule1.alf.es.bw.schule.de
schule1.alf.es.bw.schule.de"
```

Es werden **alle** drei Einträge benötigt! Wenn beim Versand von E-Mail nur ein Benutzername als Empfänger angegeben wird (z.B. `weber`), wird der `localhost`-Eintrag benötigt. Die beiden anderen Eintrage werden benötigt, um, unabhängig von der Schreibweise einer vollständigen E-Mail-Adresse der lokalen Domäne, diese auch lokal zuzustellen, und nicht an BelWü weiterzuleiten.

- * E-Mail weiterleiten (optional)

Wenn Sie in Ihrem lokalen Netz ein weiteres E-Mailsystem verwenden (z.B. von Novell NetWare oder Microsoft), dann können alle Mails anstelle der lokalen Zustellung an den entsprechenden Mail-Server weitergeleitet werden. Der zugehörige Eintrag könnte lauten:

```
SENDMAIL_RELAY="10.0.0.200"
```

- Argumente beim Start von *sendmail*

Sendmail wird beim Booten des Rechners mit den angegebenen Argumenten gestartet:

```
SENDMAIL_ARGS="-bd -q30m -om"
```

Dabei bedeutet `–bd`, dass *sendmail* im Dämon-Modus gestartet wird, so dass E-Mail über das TCP/IP-Netzwerk von anderen Rechnern akzeptiert wird.
Mit `–q30m` schaut *sendmail* alle 30 Minuten nach, ob im Queue-Verzeichnis `/var/mqueue` noch E-Mail liegt, die ausgeliefert werden muss.

- Aktualisieren der Konfiguration

Wenn Sie die erforderlichen Parameter in der Datei `/etc/rc.config` eingetragen haben, müssen Sie `SuSEconfig` aufrufen, damit automatisch eine neue *sendmail*-Konfigurationsdatei `/etc/sendmail.cf` generiert wird:

**SuSEconfig [↵]**

Sinnvollerweise starten Sie danach Ihren Linux-Server neu.

---


**Übung 13-1:** Konfiguration des Linux Mail-Servers

---

## 13.4 Konfiguration des E-Mail-Clients *Netscape Messenger*

Damit Sie von Ihrer Windows 95-Workstation E-Mail empfangen, schreiben und versenden können, muss der Mail-Client korrekt konfiguriert sein. In dieser Schulung wird als Mail-Client der *Netscape Messenger* verwendet, der im Programmpaket *Netscape Communicator* enthalten ist.

- Anlegen eines neuen Benutzerprofils

Sie können mit dem *Netscape Communicator* auf jeder Workstation verschiedene sog. *Benutzerprofile* einrichten, in denen individuelle Einstellungen abgespeichert werden.

Beenden Sie ggf. zuerst Netscape und starten Sie den *User Profile Manager* über **Start → Programme → Netscape Communicator → Utilities → User Profile Manager**.

Klicken Sie auf der Seite *Select a profile* auf **New** und geben Sie alle erforderlichen Parameter ein. Weitere Details finden Sie in der nachfolgenden Übung.

Sind mehrere Benutzerprofile vorhanden, wird man beim Start des *Netscape Communicators* aufgefordert, ein Profil auszuwählen. Alternativ kann der *Netscape Communicator* mit einem Benutzerprofil als Parameter gestartet werden. Hierfür müssen Sie die "Verknüpfung mit Netscape Communicator" erweitern um den Eintrag *–P"Profilname"*. Um z.B. das Profil des Benutzers weber zu verwenden, wäre der korrekte Eintrag

```
C:\Programme\Netscape\Communicator\Program\netscape.exe -P"weber"
```

Beachten Sie **unbedingt** die Syntax, denn es darf sich zwischen `P` und `"` kein Leerzeichen befinden!

- Start des Netscape Messengers

Sie können den *Netscape Messenger* entweder direkt starten über **Start → Programme → Netscape Communicator → Netscape Messenger** oder durch Aufruf des Netscape-Navigators und Klicken auf das Mail-Symbol. Wenn mehrere Profile auf Ihrer Workstation vorhanden sind, müssen Sie vorher ein Profil auswählen.

**Übung 13-2:** Konfiguration des E-Mail-Clients Netscape Messenger

### Zusammenfassung

Ein wesentlicher Internet-Dienst ist der E-Maildienst, mit dem Benutzer elektronische Briefe sowie Daten aller Art austauschen können. Sie benötigen hierfür einen Mail-Server und pro Benutzer/Arbeitsplatz einen Mail-Client.

Der Mail-Server ist für die korrekte Zustellung der E-Mail verantwortlich und leitet sie ggf. vom LAN ins Internet bzw. umgekehrt. Er kommuniziert dabei mit einem Mail Relay Host im Internet. SuSE-Linux beinhaltet als Mail-Server das Paket *sendmail*, das automatisch mitinstalliert wird und nur noch konfiguriert werden muss.

Der Mail-Client wird zum Lesen, Schreiben und Beantworten von E-Mails benötigt. Mit dem *Netscape Messenger* aus dem Programmpaket *Netscape Communicator* steht ein kostenloser Client zur Verfügung

# 14 News

News bieten die Möglichkeit zum Informationsaustausch in thematisch sortierten Diskussionsforen. Die Bereitstellung dieser Diskussionsforen übernimmt ein News-Server, während zum Lesen und Schreiben von News ein Newsclient benötigt wird. Ihre Linux-Installation enthält bereits den News-Server InterNetNews *inn*, der nur noch konfiguriert werden muss. Einen News-Client stellt Ihnen das Programmpaket Netscape Communicator zur Verfügung.

Der News-Server wird im Rahmen dieser Schulung nicht voll funktionsfähig sein: es findet keine Kommunikation mit anderen News-Servern statt. Grund hierfür ist der enorme Datenbestand, der über Ihre Telefonleitung zum Provider ausgetauscht werden müsste. Dieser würde Ihre ohnehin schon langsame Wählverbindung belasten und die Telefongebühren in die Höhe treiben. Dennoch wird Ihren Schülern die Möglichkeit gegeben, lokal zu diskutieren.

Wenn Sie einen vollwertigen News-Server verwenden wollen, lesen Sie bitte die Hinweise, die Sie unter `/usr/doc/packages/i4ldoc/leafsite/index.html` im Kapitel "Das Usenet offline bearbeiten" finden.

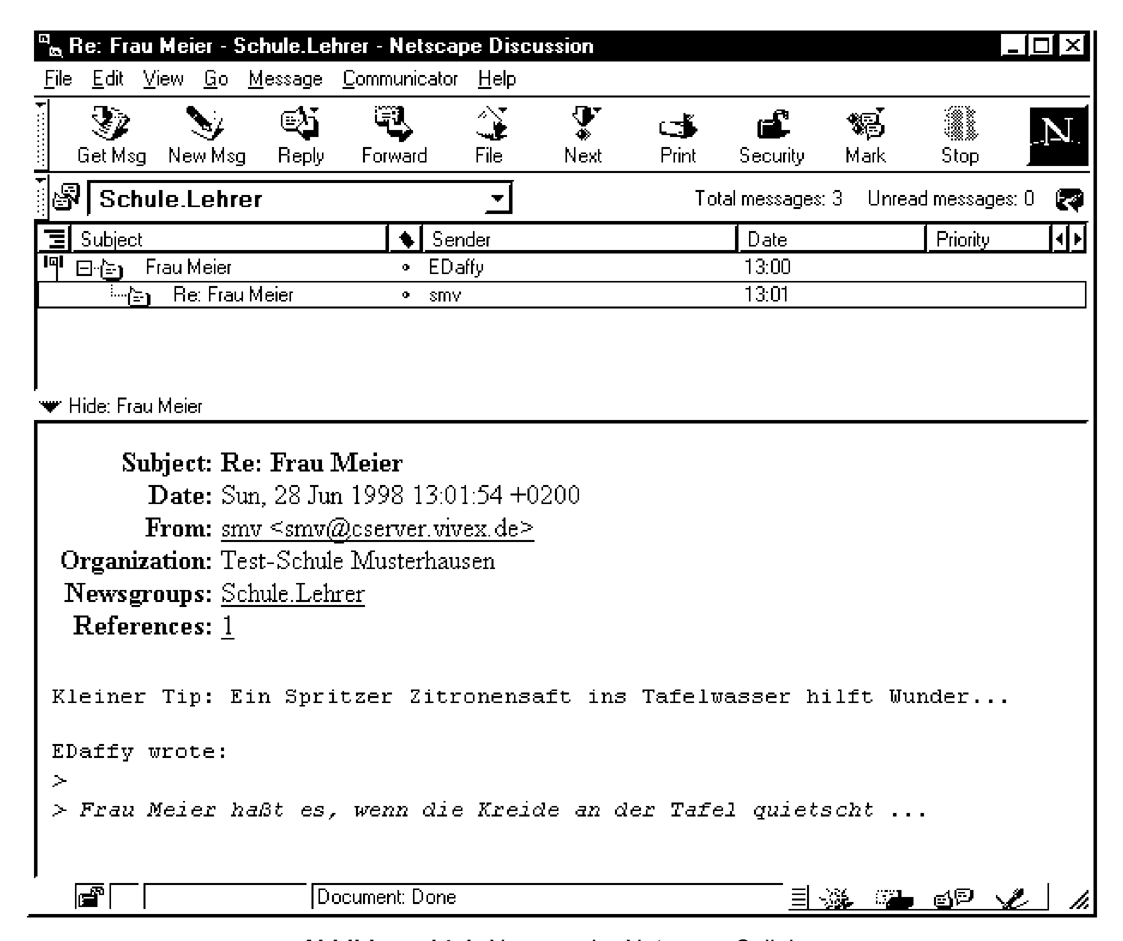
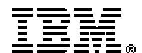



**Abbildung 14-1:** Newsreader Netscape Collabra



## 14.1 Überblick

Beim Einsatz von News-Servern wird üblicherweise das NNTP-Protokoll (Network News Transfer Protocol) verwendet. Bei diesem Protokoll wird der Transfer von Artikeln interaktiv zwischen den News-Systemen vereinbart, so dass ein Mehrfachtransport von Artikeln minimiert wird, d.h. die Übertragung erfolgt fast verzögerungsfrei.

Nach dem Aufbau einer Verbindung verständigen sich News-Client und -Server mit bestimmten Befehlen. Zum einen können spezielle Transfer-Clients den Server ansprechen, um die News zu einem weiteren Server zu transportieren. Zum anderen können die Newsreader auf PCs in einem lokalen Netzwerk einen News-Server ansprechen, um News zu lesen oder zu senden ("posten").

Die Übertragung der News ist mit zwei unterschiedlichen Verfahren möglich. Beim Pushing (engl. Schieben) bietet der Server dem Client einen News-Artikel an, den dieser annehmen oder ablehnen kann. Dieses Verfahren erzeugt allerdings eine relativ hohe Last auf dem Server. Mittels Pulling (engl. Ziehen) fordert der Client beim Server eine Liste aller verfügbaren Artikel an. Nach Eingang der Liste wählt der Client die Artikel aus, die noch nicht vorhanden sind und fordert diese Artikel an.

## 14.2 Installation des News-Servers INN

Wenn Sie bei der Linux-Installation die Konfiguration *Internet access server* gewählt haben, ist bereits das Paket ***inn*** aus der Paketserie ***n*** installiert. Für den automatischen Start des News-Servers muss die Umgebungsvariable `START_INN` in der Datei `/etc/rc.config` auf `yes` gesetzt werden. Konfigurieren Sie anschließend den News-Server und starten Sie Ihren Rechner neu.

Sie finden viele Informationen (FAQs) im Verzeichnis:

`/usr/doc/packages/inn`

welche im komprimierten "gz"-Format vorliegen.

Zum Entkomprimieren geben Sie ein:

**gunzip /usr/doc/packages/inn/*.gz [↵]**

Ferner finden Sie einen kurzen Überblick über die Installation in der Datei:

`/var/lib/news/README.linux`

## 14.3 Konfiguration des News-Servers

Die Konfiguration eines News-Servers kann beliebig kompliziert werden. Für Ihren Schulbetrieb ist es jedoch ausreichend, einen minimal konfigurierten News-Server zu betreiben.

### 14.3.1 Konfigurationsdateien

Der News-Server *inn* wird über folgende Dateien im Verzeichnis `/var/lib/news` konfiguriert:

- `inn.conf` Allgemeine Konfigurationsdatei
- `control.ctl` Zugangskontrolle für sog. Control-Messages
- `expire.ctl` Regelt die Gültigkeitsdauer von Newsgroups
- `hosts.nntp` Erlaubt den angegebenen Rechnern das Zustellen von news
- `newsfeeds` Legt fest, wohin Usenet-Artikel gesendet werden
- `nnrp.access` Zugriffskontrolle für lokalen News-Server

Ferner finden Sie die Dateien:

- `active` Liste aller Newsgroups auf Ihrem Server
- `newsgroups` Beschreibung der Newsgroups

### 14.3.2 Minimalkonfiguration

Folgende Schritte sind notwendig, um einen minimal konfigurierten News-Server (kein Kontakt zu anderen News-Servern, siehe Einleitung) zu betreiben:

- Editieren der Datei `/etc/`**`rc.config`**

Damit der News-Server bei jedem Booten des Linux-Servers automtisch startet, muss die Variable `START_INN` auf den Wert `yes` gesetzt werden:

```
START_INN=yes
```

- Editieren der Datei `/var/lib/news/`**`inn.conf`**

Tragen Sie den Namen Ihrer Schule in den Parameter `organization` ein. Dieser wird beim Zugriff von Clients auf den News-Server im Feld *Organization* angezeigt:

```
organization:   Test-Schule Musterhausen
```

- Editieren der Datei `/var/lib/news/`**`nnrp.access`**

Diese Datei regelt den Zugriff auf Ihren News-Server. Einträge haben die Form

```
<Rechnername oder IP-Adresse>:<Art des Zugriffs>:<Benutzername, der
vor dem Posten von Artikeln anzugeben ist>:<Passwort, das vor dem
Posten von Artikeln anzugeben ist>:<Newsgroups, die gelesen werden
dürfen>
```

Erlauben Sie allen Clients in Ihrem LAN den Zugriff auf Ihren News-Server. Gestatten Sie sowohl das Lesen (Read), als auch das Schreiben (Post) von allen Artikeln ohne Zugriffskontrolle. Wenn Sie einen **vollwertigen** Name-Server für Ihre Domäne installiert haben (siehe Kap. 7.3), lautet für die Domäne schule1.alf.es.bw.schule.de der entsprechende Eintrag:

```
*.schule1.alf.es.bw.schule.de:Read Post:::*
```

Andernfalls kann Ihr Name-Server nicht die Namen der anfragenden Arbeitsstationen auflösen, da sie weder ihm, noch dem Name-Server des Providers (BelWü) bekannt sind. Sie benötigen in diesem Fall den allgemeinen Eintrag:

```
*:Read Post:::*
```

- Anlegen der Newsgroups

Jede Diskussionsgruppe (Newsgroup), die Sie anlegen wollen, benötigt einen Eintrag in der Datei `/var/lib/news/active`. Hier werden alle zur Verfügung stehenden Newsgroups aufgeführt. Sie finden bereits die System-Gruppen `control`, `control.cancel` und `junk`. Neueinträge haben die Form

```
Name 0000000000 0000000000 y
```

Fügen Sie weitere Newsgroups hinzu. Obwohl dies manuell über einen Editor erfolgen kann, sollten Sie besser das zugehörige Kommando `/usr/lib/news/bin/ctlinnd newgroup` verwenden: Viele Probleme mit dem *inn* sind auf Syntax-Fehler in den Konfigurationsdateien zurückzuführen! Fügen Sie z.B. die Newsgroups `Schule.Lehrer`, `Schule.Schueler` und `Schule.Unterrichtsfaecher` hinzu. Die zugehörigen Kommandos lauten:

```
/usr/lib/news/bin/ctlinnd newgroup Schule.Lehrer
/usr/lib/news/bin/ctlinnd newgroup Schule.Schueler
/usr/lib/news/bin/ctlinnd newgroup Schule.Unterrichtsfaecher
```



Sie finden daraufhin in der Datei `/var/lib/news/active` die neuen Einträge

```
Schule.Lehrer 0000000000 0000000000 y
Schule.Schueler 0000000000 0000000000 y
Schule.Unterrichtsfaecher 0000000000 0000000000 y
```

---

***Achtung:*** *Verwenden Sie keine Umlaute oder Sonderzeichen für die Namen Ihrer Newsgroups, andernfalls können diese Gruppen nicht verwendet werden!*

---

Wenn Sie Newsgroups löschen wollen, verwenden Sie das Kommando:

```
/usr/lib/news/bin/ctlinnd rmgroup Name_der_Newsgroup
```

und für eine Auflistung der vorhandenen Newsgroups:

```
/usr/lib/news/bin/getlist –h localhost
```

- Editieren der Datei `/var/lib/news/`**`newsgroups`**

Hier können Sie eine Beschreibung der jeweiligen Newsgroups eintragen. Für oben genanntes Beispiel könnte dies sein:

```
Schule.Lehrer                 Lob und Beschwerden über Lehrer
Schule.Schueler               Der neueste Klatsch und Tratsch
Schule.Unterrichtsfaecher     Was gibt's neues?
```

- Rechner neu starten

Damit Ihre Änderungen gültig werden, starten Sie am besten den Linux-Server neu. Sie können auch `/sbin/init.d/inn stop` und danach wieder `/sbin/init.d/inn start` eingeben.

---



**Übung 14-1:** Konfiguration des News-Servers INN

---

## 14.4 Konfiguration der News-Clients

Im Programmpaket Netscape Communicator ist der Newsreader *Netscape Collabra* enthalten. Damit ein Client auf den News-Server zugreifen kann, muss der News-Server in den Voreinstellungen eingetragen sein. Diese sind über **Edit → Preferences... → Mail & Groups → Groups Server** zu erreichen.

Ferner muss jeder Client ein **E-Mail-Account** besitzen, da Antworten auf News grundsätzlich sowohl in die betreffenden Newsgroup, als auch direkt zum Verfasser per E-Mail gesendet werden können. Ebenso ist ein Benutzerkonto notwendig, wenn Sie eine Zugangskontrolle eingerichtet haben.

Jedes Diskussionsforum (Newsgroup), zu dem ein Client Zugang wünscht, muss von ihm **abonniert** werden. Sie finden hierfür auf der Collabra-Startseite *Netscape Message Center* den (oder die) eingetragenen News-Server. Ein Rechtsklick auf den News-Server öffnet ein Kontextmenü mit dem Eintrag **Subscribe to Discussion Groups ...** Im nachfolgenden Fenster können Sie aus den zur Verfügung stehenden Diskussionsforen die für Sie interessanten auswählen.

Durch einen Doppelklick auf ein abonniertes Diskussionsforum öffnet sich das Fenster *Netscape Discussion*, in dem alle Beiträge und eventuell vorhandene Antworten aufgelistet werden. Das Lesen und Beantworten von News geschieht völlig analog zur E-Mail.

---



**Übung 14-2:** Konfiguration des Newsclients Netscape Collabra

---

# 15 Exkurs: Kernelkonfiguration

Der **Kernel**, der nach der Installation auf die Diskette geschrieben wird (und auch im installierten System im `root`-Verzeichnis zu finden ist), ist so konfiguriert, dass er ein möglichst breites Spektrum von Hardware unterstützt. Dieser Kernel ist demnach nicht speziell auf Ihr System abgestimmt, so dass das Booten unnötig Zeit in Anspruch nimmt: Der Kernel versucht, die konfigurierte Hardware zu erkennen, obwohl sie nicht vorhanden ist. Ferner wird einiges an Hauptspeicher verschwendet, da überflüssige Treiber im Kernel vorhanden sind.

Somit ist es von Vorteil, einen eigenen Kernel, abgestimmt auf das eigene System, zu generieren. Darüberhinaus ermöglicht das "Selberbauen" des Kernels in einigen Fällen erst die Verwendung bestimmter Hardware, wie z.B. exotischer Busmäuse oder Soundkarten. Und nicht zuletzt gestattet das Konfigurieren des Kernels einen höchst interessanten Einblick in den gegenwärtigen Stand der Entwicklung.

Für das Erzeugen eines neuen Kernels existieren bereits sog. *Makefiles* des C-Compilers, mit deren Hilfe der Ablauf fast völlig automatisiert ist, Lediglich die Abfrage der vom Kernel zu unterstützenden Hardware muss interaktiv durchlaufen werden.

Die Kernelquellen befinden sich im Verzeichnis `/usr/src/linux`. Sollten Sie vorhaben, am Kernel herumzuexperimentieren, um verschiedene Versionen des Kernels gleichzeitig auf der Platte zu haben, so bietet es sich an, die einzelnen Versionen in verschiedene Unterverzeichnisse zu entpacken und die augenblicklich relevante Quelle über einen Link anzusprechen. Diese Form der Installation wird von `Yast` automatisch vorgenommen.

Genauergenommen können die Kernel-Quellen in einem beliebigen Unterverzeichnis installiert und übersetzt werden. Da es jedoch eine Ganze Reihe von Software gibt, die die Kernelquelle unter `/usr/src/linux` erwartet, sollte dieses Verzeichnis gewählt werden, um ein fehlerfreies Compilieren von systemnahen Programmen zu gewährleisten.

## 15.1 Konfiguration des Kernels

Um einen neuen Kernel kompilieren zu können, müssen folgende Pakete aus der Serie ***d*** *(Development)* installiert werden:

- `gcc` C-Compiler
- `lx_suse` Kernel-Quellen
- `binutils` GNU Binutils
- `libc` Include-Dateien für den C-Compiler
- `make`

**Achtung:** Diese Pakete sind in der installierten Konfiguration *Internet access server* ***nicht*** enthalten!!!

Die Konfiguration des Kernels kann man auf drei verschiedene Arten vornehmen:

- Auf der Kommandozeile
- Im Menü im Textmodus
- Im Menü unter Xwindows

In dieser Unterlage wird ausschließlich das *Menü im Textmodus* verwendet. Nähere Informationen über die anderen Verfahren finden Sie im Linux-Handbuch und diverser Literatur.

Sie starten die Konfiguration, indem Sie zuerst in das Verzeichnis `/usr/src/linux` wechseln:

**cd /usr/src/linux [↵]**

Anschließend wird das Konfigurationsprogramm mit dem Befehl:

**make menuconfig [↵]**

gestartet. Nach Starten des Konfigurationsprogramms befinden Sie sich im Hauptmenü und können zu unterschiedlichen Kategorien Einstellungen verändern. Die wichtigsten Netzwerkeinstellungen können Sie unter <`Networking options`> wiederum durch Cursorbewegungen verändern.

Nachdem Sie die Kernel-Einstellungen für Ihre Gegebenheiten konfiguriert haben, müssen Sie mit Auswahl von <`EXIT`> das Programm beenden.

Anschließend starten Sie mit den Befehlen `make dep`, `make clean` und `make zImage` die Übersetzung (Compilierung). Diese 3 Befehle können Sie auch in einer Befehlszeile eingeben, so dass sie hintereinander abgearbeitet werden. Dies birgt Vorteile in sich, wenn Sie die Kernel-Compilierung automatisch, z.B. „über Nacht“, durchführen lassen wollen. Geben Sie dafür ein:

**make dep clean zImage [↵]**

Je nach Leistung Ihres Systems dauert es jetzt ca. 4 Minuten (schneller mit PentiumPro) bis zu einigen Stunden (bei 386ern mit 8 MB), bis der Kernel neu übersetzt ist. Während der Übersetzungsprozedur können Sie sich selbstverständlich auf einer anderen Konsole weiterhin mit dem System beschäftigen.

Nach der erfolgreichen Übersetzung finden Sie den komprimierten Kernel im Verzeichnis:

```
/usr/src/linux/arch/i386/boot
```



Das Kernel-Image (= Datei, die den Kernel enthält) heißt `zImage`. Finden Sie diese Datei nicht vor, ist aller Wahrscheinlichkeit noch ein Fehler während der Kernelübersetzung aufgetreten. Dies geht leicht in der Menge der Bildschirmangaben unter. Ob ein Fehler aufgetreten ist, können Sie dadurch verifizieren, dass Sie nochmals die Kernelübersetzung anstoßen und auf entsprechende Fehlermeldung achten:

**make zImage [↵]**

Aber keine Angst: Fehler bei der Kernleübersetzung treten eher selten auf!

Wenn Sie Teile des Kernels als ladbare Module konfiguriert haben, müssen Sie anschließend das Übersetzten dieser Module veranlassen. Dies erreichen Sie durch:

**make modules [↵]**

Wurden die von Ihnen gewünschten Module erfolgreich erzeugt, können Sie sie durch Eingabe von:

**make modules_install [↵]**

in die korrekten Zielverzeichnisse (`/lib/modules/<Version>`) kopieren lassen.

Nachdem Sie den Kernel übersetzt haben, müssen Sie dafür sorgen, dass er künftig gebootet wird. Verwenden Sie den LILO, so muss dieser neu installiert werden. Im einfachsten Fall kopieren Sie dazu den neuen Kernel nach `/vmlinuz` und rufen einfach den LILO auf:

**lilo [↵]**

Um sich vor unliebsamen Überraschungen zu schützen, empfiehlt es sich jedoch, den alten Kernel beizubehalten, um ihn notfalls booten zu können, wenn der neue Kernel nicht wie erwartet funktioniert.

Tragen Sie in Ihrer `/etc/lilo.conf` zusätzlich ein Label `/vmlinuz.old` als Boot-Image ein und benennen Sie den alten Kernel nach `/vmlinuz.old` um. So stellen Sie sicher, dass Sie immer noch mit dem vorherigen Kernel booten können, falls dies mit dem neuen nicht funktionieren sollte.

Haben Sie die Datei `/ect/lilo.conf` nach Ihrem Wünschen angepasst, so können Sie mit:

**make zlilo [↵]**

die Installation des LILO nach dem Übersetzten der Kernels auch automatisch durchführen lassen.

Falls Sie Linux von DOS aus über `linux.bat` (also mit `loadlin`) starten, müssen Sie den neuen Kernel noch nach `/dosc/loadlin/zimage` kopieren, damit er beim nächsten Booten wirksam werden kann.

Weiterhin ist folgendes zu beachten: Die Datei `/System.map` enthält die Kernelsymbole, die die Kernelmodule benötigen, um Kernelfunktionen korrekt aufrufen zu können. Diese Datei ist abhängig vom aktuellen Kernel. Daher sollten Sie die aktuelle Datei `/usr/src/linux/System.map` nach der Übersetzung und Installation des Kernels in das Hauptverzeichnis kopieren. Falls Sie Ihre Kernel mittels **make zlilo** erstellen, wird diese Aufgabe automatisch für Sie erledigt.

Sollten Sie beim Booten eine Fehlermeldung wie „`System.map does not, match actual kernel`" erhalten, wurde wahrscheinlich nach der Kernelübersetzung die Datei `System.map` nicht nach `/` kopiert.

## Bootdisk erstellen

Möchten Sie eine Boot-Diskette mit dem neuen Kernel erstellen, so können Sie einfach den folgenden Befehl verwenden:

**make zdisk [↵]**

## Festplatte nach der Kernel-Übersetzung aufräumen

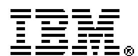
Sie können die während der Kernel-Übersetzung erzeugten Objekt-Dateien löschen, falls Sie Probleme mit dem Plattenplatz haben:

**cd /usr/src/linux [↵]**
**make clean [↵]**

Falls Sie jedoch über ausreichend Plattenplatz verfügen und vorhaben, den Kernel des öfteren neu zu konfigurieren, so überspringen Sie diesen letzten Schritt. Ein erneutes Compilieren des Kernels ist dann erheblich schneller, da nur die Teile des Systems neu übersetzt werden, die von den entsprechenden Änderungen betroffen sind.

# 16 Stichwortverzeichnis





## F



## H



## I



## K



## L



## M



## N



## O



## P


Multimedi@
Schule